07.057

Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit

(BWIS)

(Besondere Mittel der Informationsbeschaffung)

vom 15. Juni 2007

Sehr geehrte Frau Nationalratspräsidentin
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen einen Entwurf betreffend die Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit mit dem Antrag auf Zustimmung.

Wir versichern Sie, sehr geehrte Frau Nationalratspräsidentin, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

15. Juni 2007

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Micheline Calmy-Rey
Die Bundeskanzlerin: Annemarie Huber-Hotz

Übersicht

Das Bundesgesetz vom 21. März 1997[1] *über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) trat am 1. Juli 1998 in Kraft und dient der Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz sowie dem Schutz der Freiheitsrechte ihrer Bevölkerung.*

Das rechtzeitige Erkennen von gegen die Sicherheit der Schweiz gerichteten Gefahren verlangt eine ständige Beurteilung der Gefährdungslage. Bundesrat und Parlament, aber auch die Kantone sollen existenzbedrohende Gefahren frühzeitig erkennen, in ihre Sicherheitspolitik miteinbeziehen und rechtzeitig Gegenmassnahmen treffen können. In der zeitgerechten Bereitstellung der dazu notwendigen Informationen besteht die erste Aufgabe des präventiven Staatsschutzes (Sicherheitspolitischer Bericht 2000, Seiten 32 und 54).

Jede Risikoanalyse verlangt vielfältige Informationen und ein solides Informationsnetz. Die Beschaffung sicherheitsrelevanter Informationen ist eine nachrichtendienstliche Aufgabe. Für die Beschaffung dieser Informationen über das Inland ist der Dienst für Analyse und Prävention (DAP) im Bundesamt für Polizei zuständig. Seine Aufgabe ist u.a. die frühzeitige Erkennung von Gefährdungen durch Terrorismus, verbotenen Nachrichtendienst, gewalttätigen Extremismus, verbotenen Handel mit Waffen und radioaktiven Materialien und verbotenen Technologietransfer (Proliferation). Dazu müssen auch vertrauliche Informationen beschafft werden.

Die Sicherheits- und Gefahrenlage der Schweiz hat sich in den letzten Jahren namentlich durch die erhöhte Wahrscheinlichkeit von islamistisch motivierten Terroranschlägen sukzessive verschlechtert. Seit längerer Zeit können die Nachrichtenbedürfnisse für die Lagebeurteilung und Entscheidfindung, aber auch für die rechtzeitige Erkennung verborgener Gefahren nicht mehr ausreichend befriedigt werden. Das nachrichtendienstliche Abwehrdispositiv weist Lücken auf und genügt der heutigen Gefahrenlage nicht mehr. Die Lücken können weder durch das konsequente Ausschöpfen bestehender Möglichkeiten noch durch eine Verbesserung des Informationsflusses und der Koordination zwischen Nachrichtendienst und Strafverfolgung noch durch den Ausbau des formellen und materiellen Strafrechts geschlossen werden. Erforderlich ist vielmehr eine beschränkte, aber gezielte und streng überwachte Verbesserung der nachrichtendienstlichen Informationsbeschaffung. Sie soll effektiv gestaltet und dem europäischen Standard angenähert werden.

Dazu werden insbesondere folgende Massnahmen getroffen:

– *Beschränkt auf die Abwehr schwerer Gefährdungen (Terrorismus, verbotener politischer und militärischer Nachrichtendienst sowie verbotener Handel mit Proliferationsgütern) sollen die Behörden und Verwaltungseinheiten des Bundes und der Kantone in konkreten Fällen zur Auskunftserteilung verpflichtet werden. Unter den gleichen Voraussetzungen sollen auch*

[1] SR **120**

gewerbliche Transporteure über bereits vorhandene Daten auskunftspflichtig werden.

– *Als letztes Mittel sollen besondere Mittel zur Informationsbeschaffung eingesetzt werden können. Wiederum beschränkt auf die Bereiche Terrorismus, verbotenen politischen oder militärischen Nachrichtendienst und Proliferation soll bei konkreten Gefährdungslagen das präventive Überwachen des Post- und Fernmeldeverkehrs, das Beobachten von gefährlichen Personen an nicht allgemein zugänglichen Orten, auch mittels technischem Überwachungsgerät, sowie das geheime Durchsuchen von Datenbearbeitungssystemen zulässig sein. Der Einsatz dieser Mittel wird einer doppelten Bewilligungspflicht unterstellt (richterliche Prüfung durch das Bundesverwaltungsgericht, Prüfung nach staatspolitischen Gesichtspunkten durch die Vorsteher oder Vorsteherinnen des EJPD und des VBS).*

– *Der Vorsteher oder die Vorsteherin des EJPD soll die Kompetenz erhalten, Tätigkeiten zu verbieten, die terroristische oder gewaltextremistische Umtriebe fördern und die innere oder äussere Sicherheit der Schweiz konkret gefährden. Weiter sollen die Inanspruchnahme von Informantinnen und Informanten, ihr Schutz und ihre Entschädigung auf eine formellgesetzliche Grundlage gestellt werden. Um bei der Informationsbeschaffung den Schutz von Informanten und Informantinnen sowie von Mitarbeiterinnen und Mitarbeitern des DAP sicherzustellen, wird auch die Möglichkeit zur Legendierung (Tarnidentitäten) geschaffen.*

– *Mit diesen erweiterten Kompetenzen geht eine gleichwertige Stärkung des Rechtsschutzes einher: Nicht nur unterliegt die Anordnung von Mitteln der besonderen Informationsbeschaffung einer kumulativen Prüfung durch Bundesverwaltungsgericht und Exekutive, sondern auch die Entscheide über die Mitteilungspflicht und die Anordnung von Tätigkeitsverboten unterliegen einer wirksamen richterlichen Kontrolle durch Bundesverwaltungs- und Bundesgericht.*

Eine unrechtmässige Beeinträchtigung von Grundrechten unbeteiligter Personen wird durch die einschränkenden Kriterien und die mehrfachen Kontrollen verhindert.

Alle Massnahmen sind verfassungskonform und mit den Grundrechten vereinbar, beruhen namentlich auf einem ausgewiesenen öffentlichen Interesse und wahren den Grundsatz der Verhältnismässigkeit. Auch steht die Vorlage im Einklang mit der EMRK und dem Internationalen Pakt über bürgerliche und politische Rechte.

Die für die Umsetzung erforderlichen Stellen, Investitionen und Betriebskosten werden vom EJPD intern kompensiert.

Inhaltsverzeichnis

Übersicht **5038**

Abkürzungsverzeichnis **5042**

1 Grundzüge der Vorlage **5044**

1.1 Ausgangslage 5044
1.1.1 Entstehungsgeschichte der Vorlage 5044
1.1.2 Dienst für Analyse und Prävention (DAP): Ziviler Inlandnachrichtendienst 5045
1.1.3 Weitere Aufgaben und Zuständigkeiten im Bereich der Sicherheit 5048
1.1.4 Informationsaustausch und Zusammenarbeit mit anderen Behörden 5051
1.1.5 Tabellarische Übersicht 5054
1.1.6 Sicherheitslage der Schweiz 5055
1.1.7 Zusammenwirken von Nachrichtendienst und Strafverfolgung 5061
1.1.8 Beurteilung der Risikofelder 5063
1.2 Untersuchte Lösungsmöglichkeiten 5065
1.2.1 Konsequentes Ausschöpfen bestehender Möglichkeiten im Bereich des Strafrechts und des präventiven Staatsschutzes 5065
1.2.2 Verbesserung des Informationsflusses und der Koordination zwischen Repression und Prävention 5065
1.2.3 Ausbau des formellen und materiellen Strafrechts 5066
1.2.4 Ausbau des präventiven Staatsschutzes 5066
1.2.5 Weitere Gesetzgebungsprojekte 5067
1.3 Die beantragte Neuregelung 5068
1.4 Begründung und Bewertung der vorgeschlagenen Lösung 5069
1.4.1 Ergebnis des Vernehmlassungsverfahrens 5070
1.4.2 Überarbeitung des Vorentwurfes 5071
1.5 Abstimmung von Aufgaben und Finanzen 5072
1.6 Rechtsvergleich und Verhältnis zum europäischen Recht 5073
1.6.1 Allgemeines 5073
1.6.2 Rechtsvergleich mit dem Ausland 5074
1.6.3 Rechtsschutz und institutionelle Kontrollen im Ausland 5074
1.6.4 Vergleich mit der Schweiz 5075
1.7 Umsetzung 5076
1.8 Erledigung parlamentarischer Vorstösse 5076

2 Erläuterungen zu den einzelnen Artikeln **5076**

3 Auswirkungen **5119**

3.1 Auswirkungen auf den Bund 5119
3.1.1 Finanzielle Auswirkungen 5119
3.1.2 Personelle Auswirkungen 5119
3.1.3 Sonstige Auswirkungen 5120
3.2 Auswirkungen auf Kantone und Gemeinden 5120
3.3 Auswirkungen auf die Volkswirtschaft 5120

3.3.1 Notwendigkeit und Möglichkeit staatlichen Handelns 5120
3.3.2 Auswirkungen auf die einzelnen gesellschaftlichen Gruppen 5121
3.3.3 Auswirkungen auf die Gesamtwirtschaft 5121
3.3.4 Alternative Regelungen 5121
3.3.5 Zweckmässigkeit im Vollzug 5121
3.4 Andere Auswirkungen 5121
3.4.1 Auswirkungen auf die Aussenpolitik 5121
3.4.2 Auswirkungen auf die internationalen Beziehungen 5122

4 Verhältnis zur Legislaturplanung 5122

5 Rechtliche Aspekte 5122

5.1 Verfassungsmässigkeit 5122
5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz 5123
5.3 Erlassform 5124
5.3.1 Gesetzesform 5124
5.3.2 Teilrevision 5124
5.4 Unterstellung unter die Ausgabenbremse 5124
5.5 Vereinbarkeit mit dem Subventionsgesetz 5124
5.6 Delegation von Rechtsetzungsbefugnissen 5125

Anhang: Rechtsvergleich (Deutschland, Österreich, Frankreich, Italien, Luxemburg, Niederlande, EU) 5126

Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (Besondere Mittel der Informationsbeschaffung) *(Entwurf)* **5139**

Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
BA	Bundesanwaltschaft
BBl	Bundesblatt
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BKP	Bundeskriminalpolizei
BSD	Bundessicherheitsdienst
BStP	Bundesgesetz vom 15. Juni 1934 über die Bundesstrafrechtspflege (SR *312.0*)
BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR *780.1*)
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR *101*)
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (SR *120*)
DAP	Dienst für Analyse und Prävention
DBA	Dienst für Besondere Aufgaben im Generalsekretariat UVEK
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR *235.1*)
E-StPO	Entwurf zur Schweizerischen Strafprozessordnung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EKF	Abteilung Elektronische Kriegsführung im VBS
EMRK	Europäische Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (SR *0.101*)
EU	Europäische Union
Europol	Europäisches Polizeiamt
fedpol	Bundesamt für Polizei
Interpol	Internationale Kriminalpolizeiliche Organisation
IRSG	Bundesgesetz vom 20. März 1981 über die internationale Rechtshilfe in Strafsachen (SR *351.1*)
i.V.m.	in Verbindung mit
MG	Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung (SR *510.10*)
OK	organisierte Kriminalität
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR *311.0*)
StPO	Schweizerische Strafprozessordnung (BBl *2006* 1389)
UNO	Organisation der Vereinten Nationen
UVEK	Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VEKF	Verordnung vom 15. Oktober 2003 über die elektronische Kriegsführung (SR *510.292*)

VWIS	Verordnung vom 27. Juni 2001 über die Wahrung der inneren Sicherheit (SR *120.2*)
ZentG	Bundesgesetz vom 7. Oktober 1994 über kriminalpolizeiliche Zentralstellen des Bundes (SR *360*)
ZentV	Verordnung vom 30. November 2001 über die Wahrnehmung Kriminalpolizeilicher Aufgaben im Bundesamt für Polizei (SR *360.1*)

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage

1.1.1 Entstehungsgeschichte der Vorlage

Der Inlandnachrichtendienst weist seit mehreren Jahren auf Mängel bei der präventiven Gefahrenabwehr hin, die auf Lücken im Instrumentarium zur Aufklärung der Bedrohung zurückzuführen sind. Die Lenkungsgruppe Sicherheit und der Sicherheitsausschuss des Bundesrates (SiA) nahmen davon Kenntnis und ordneten die Prüfung geeigneter Massnahmen an.

Nach den Terroranschlägen vom 11. September 2001 wurden mehrere parlamentarische Vorstösse eingereicht. Sie fordern eine stärkere Rolle der Staatsschutzorgane und Nachrichtendienste, einen Ausbau derer Mittel und Instrumentarien sowie umfassende Berichte über die Sicherheitslage (vgl. namentlich die Motionen FDP[2], Leu[3], Merz[4] und Burkhalter[5]; die Vorstösse FDP[6] bzw. Fünfschilling[7] und Suter[8], CVP[9], Leutenegger Oberholzer[10] und Pfister[11]).

In der Folge beauftragte der Bundesrat im November 2001 das Eidgenössische Justiz- und Polizeidepartement (EJPD), ihm über Massnahmen zur Verbesserung und Bekämpfung des Terrorismus Bericht und Antrag zu unterbreiten. Im Juni 2002 hiess er den Bericht «Lage- und Gefährdungsanalyse Schweiz nach den Terroranschlägen vom 11. September 2001» gut und nahm gleichzeitig Kenntnis von der Aufteilung der Rechtsetzungsvorhaben in zwei Pakete. Das zweite Paket (d.h. die vorliegende Revision) beschlägt namentlich die Thematik des Terrorismus.

Nach vertieften Vorarbeiten und einer ersten Aussprache beauftragte der Bundesrat am 20. Oktober 2004 das EJPD, ihm im Laufe des Jahres 2005 einen Vernehmlassungsentwurf zu unterbreiten. Der Vorentwurf wurde im Juli 2005 in einer erste, und – nach Überarbeitung – im Februar 2006 in eine zweite Ämterkonsultation geschickt. Über die in den Ämterkonsultationen besonders umstrittenen Punkte sprach sich der Bundesrat am 5. April 2006 aus und beschloss das weitere Vorgehen. Auftragsgemäss wurde daraufhin ein Vernehmlassungsentwurf erarbeitet. Am 5. Juli

2 01.3545 Motion Freisinnig-demokratische Fraktion: Nachrichtendienste und Staatsschutz optimieren
3 01.3626 Motion Leu: Neue nachrichtendienstliche Kultur für neue Herausforderungen
4 01.3569 Motion Merz: Nachrichtendienste und Staatsschutz optimieren
5 04.3216 Motion Burkhalter: Terrorismusbekämpfung. Präventive Massnahmen
6 01.3552 Interpellation Freisinnig-demokratische Fraktion: Lagebeurteilung nach den Terroranschlägen
7 01.3576 Interpellation Fünfschilling: Lagebeurteilung nach den Terroranschlägen
8 01.3612 Interpellation: Terrorbekämpfung in der EU. Auswirkungen auf die Schweiz
9 01.3702 Motion Christlichdemokratische Fraktion: Fernhaltung von unter Sicherheitsaspekten unerwünschten Personen; 01.3704 Motion Christlichdemokratische Fraktion: Beseitigung von Schwachstellen in der Terrorismusprävention; 01.3705 Motion Christlichdemokratische Fraktion: Nachrichtendienst. Kooperation und Professionalität
10 01.3633 Postulat Leutenegger Oberholzer: Terroranschläge. Neue Beurteilung der Risikosituation der Schweiz
11 01.1114 Einfache Anfrage Pfister: Terroranschläge. Rasterfahndung

2006 beauftragte der Bundesrat das EJPD mit der Durchführung eines Vernehmlassungsverfahrens.

Das Vernehmlassungsverfahren dauerte vom 5. Juli bis zum 15. Oktober 2006. Bedingt durch die vielen und teilweise kontroversen Meinungen wurden dem Bundesrat vorerst der Ergebnisbericht unterbreitet und Antrag für das weitere Vorgehen gestellt. Mit Beschluss vom 4. April 2007 nahm der Bundesrat vom Ergebnis des Vernehmlassungsverfahrens Kenntnis, beauftragte das EJPD mit der Ausarbeitung der nun vorliegenden Botschaft und traf Richtungsentscheide.

1.1.2 Dienst für Analyse und Prävention (DAP): Ziviler Inlandnachrichtendienst

Aufgabe des DAP

Inlandnachrichtendienst

Der Dienst für Analyse und Prävention (DAP) im Bundesamt für Polizei (fedpol) ist der polizeiliche Inlandnachrichtendienst der Schweiz.

Die Aufgaben des DAP sind im BWIS und im dazugehörigen Verordnungsrecht geregelt. Der DAP ist beauftragt, die Staatsleitungs- und die Polizeiorgane des Bundes und der Kantone frühzeitig über Gefährdungen im Bereich der inneren Sicherheit zu informieren, damit rechtzeitig Abwehrmassnahmen getroffen werden können. Es geht dabei vor allem um Gefährdungen der Sicherheit des ganzen Landes und seiner Einwohnerinnen und Einwohner. Dazu gehören namentlich die Erkennung und Analyse von Aktivitäten schwerstkriminellen Charakters. Um diese Gefahren für die demokratischen und rechtsstaatlichen Grundlagen der Schweiz und der Freiheitsrechte und der Sicherheit der Bevölkerung rechtzeitig zu erkennen, ist der DAP zu einer permanenten Beobachtungstätigkeit sowie zu periodischen Beurteilungen der Bedrohungslage verpflichtet. Indem das BWIS die in der Regel verdeckten vorbeugenden Massnahmen und auch die daran anknüpfenden Interventionen an den Zweck bindet, staatsschutzrelevante Gefahren abzuwehren, verpflichtet es die nachrichtendienstliche Tätigkeit zu einer präventiven Zielsetzung. In Friedenszeiten nimmt der DAP auch die Aufgaben der militärischen Abwehr wahr.

Gefährdung der inneren Sicherheit

Die Wahrung der Sicherheit des Landes stellt eine originäre und primäre Staatsaufgabe dar. Sie umfasst das Sicherstellen der grundlegenden Normen des friedlichen Zusammenlebens, den Schutz der Institutionen des Staates, das Verhindern von elementaren Gefährdungen der Gesellschaft und des und der Einzelnen sowie die Abwehr sozialer Notstände[12].

Die Beurteilung, ob bestimmte Verhaltensweisen die innere Sicherheit gefährden, ist in erster Linie eine von der allgemeinen Lage abhängige politische Beurteilung. Eine Gefährdungslage ergibt sich somit nicht nur aus dem konkreten Verhalten als solchem, sondern vor allem aus dessen politischer Einbettung in das übergeordnete Umfeld. Mit anderen Worten kann dieselbe Verhaltensweise mit der Veränderung

12 Botsch. BR zum VE 96, S. 399

ihres Umfeldes von einer nicht sicherheitsrelevanten Gefahr zu einer Gefährdung der inneren Sicherheit werden oder umgekehrt.

Nimmt beispielsweise eine terroristische Organisation nach einer längeren gewaltlosen Ruhephase im heimatlichen Ausland – während dieser Zeit besteht im Regelfall nur eine latente Gefährdung der inneren Sicherheit der Schweiz – den gewaltsamen Kampf wieder auf, so können die Auswirkungen auf die Sicherheit der Schweiz rasch konkret werden. In der Praxis stehen hier im Vordergrund: Terrorakte in der Schweiz, Gewaltakte der hiesigen Diasporagemeinde untereinander, Eintreiben von «Spendengeldern» mit Druckmitteln und anschliessendem Finanztransfer ins Heimatland zur Finanzierung des Kampfes oder Rekrutierung von Mitgliedern/Kämpfern usw. Durch terroristische Akte im Ausland können zudem jederzeit Schweizerinnen und Schweizer oder schweizerische Interessen gefährdet werden.

Existenzbewahrende Dimension der Schutzaufgabe

Das permanente Beschaffen, Auswerten und Verbreiten von Nachrichten durch den DAP zielt darauf ab, die Staatslenkungsorgane über mögliche Gefährdungen des Fortbestands und der Sicherheit des Landes, der freiheitlichen Gesellschaftsordnung und der demokratischen Institutionen zu informieren.

Diese die Gesellschaft und die Nation als Ganze erfassende Dimension des Staatschutzes bringt Artikel 1 des BWIS zum Ausdruck, indem er den Staatsschutz in den Dienst der Sicherung der rechtsstaatlichen und demokratischen Grundlagen der Schweiz sowie den Schutz der Freiheitsrechte stellt.

Information der Regierung und der Öffentlichkeit

Die nachrichtendienstlichen Erkenntnisse dienen den zuständigen Behörden des Bundes und der Kantone dazu, rechtzeitig nach ihrem massgebenden Recht einzugreifen. Das Ziel der Früherkennung ist somit die Enttarnung gefährlicher Strukturen und die Aufbereitung der Erkenntnisse als Entscheidungsgrundlage für die politisch verantwortlichen Organe von Bund und Kantonen. Der Direktor des fedpol und der Chef des DAP sind ständige Mitglieder der Lenkungsgruppe Sicherheit (LGSi) und damit direkt in die Lagebeurteilung und Früherkennung der sicherheitspolitischen Führungsorgane eingebunden.

Gerade die Bekämpfung terroristischer Gefahren muss besonders früh einsetzen, um solche wenn immer möglich bereits im Stadium der Planung und Vorbereitung zu vereiteln. Dazu sind Massnahmen zur Beobachtung gefährlicher Personen und Gruppen und eine optimale internationale Zusammenarbeit notwendig. Aber selbst nach einem erfolgten Terroranschlag sind – wie ausländische Beispiele belegen – für eine rasche Identifizierung der Täterschaft nachrichtendienstliche Erkenntnisse von entscheidender Bedeutung.

Nachrichtenzyklus

Nachrichtendienste steuern ihre Tätigkeit nach den Grundsätzen des Nachrichtenzyklus. Dieser besteht aus der Planung (was interessiert?), der Beschaffung (z.B. Gespräche mit Informantinnen und Informanten), der Bewertung (z.B. Beurteilung der Vertrauenswürdigkeit einer Information), der Auswertung (z.B. Bearbeitung von Berichten und Hinweisen der Beschaffungsorgane) und der Verbreitung (z.B. Berichterstattung an die Exekutive). Eine Schwäche im Bereich der Beschaffung wirkt sich direkt auf den gesamten Zyklus aus.

Informationsbeschaffung: Jede Gefahrenanalyse und jedes darauf gestützte Handeln basieren auf vielfältigen Informationen. Nur ein Teil der nötigen Informationen kann über allgemein zugängliche Wege beschafft werden. Die Beschaffung nicht öffentlich zugänglicher Informationen ist eine zentrale Aufgabe des Nachrichtendienstes. Dabei können in die nachrichtendienstlichen Endprodukte nicht mehr und nicht bessere Informationen einfliessen, als von Gesetzes wegen überhaupt beschafft werden dürfen.

Die operationelle Informationsbeschaffung des DAP geht von der Führung besonders sensibler menschlicher Quellen bis hin zu Gegenoperationen mit enttarnten und «umgedrehten» Agenten. Viele Fälle werden zusammen mit Kantonen und/oder ausländischen Behörden bearbeitet. Daraus resultieren unverzichtbare Informationen für die Sicherheit von Bund und Kantonen.

Von besonderer Bedeutung ist der Informationsaustausch mit ausländischen Behörden. Das Meldeaufkommen umfasst jährlich ca. 20 000 Meldungen vertraulicher und geheimer Natur. Besonders wichtig ist diese internationale Zusammenarbeit auch für die Wahrnehmung fremdenpolizeilicher Aufgaben. Weist etwa Frankreich Hassprediger aus, sollen diese nicht in die Schweiz ausweichen können. Oder ist in der Schweiz ein Skinheadkonzert mit einschlägig bekannten deutschen oder italienischen Musikgruppen angesagt, sollen diese hier ihr rassistisches Gedankengut nicht öffentlich weiterverbreiten können. In beiden Fällen liegt der Erlass von Einreisesperren in der Kompetenz des DAP, der zur Prüfung der Anordnungsvoraussetzungen auf Informationen ausländischer Behörden angewiesen ist.

Bewertung der Informationen: Bei der Informationsbewertung werden die beschafften Informationen auf ihre Zuverlässigkeit hin untersucht, miteinander verglichen und in Auswerteprodukte verarbeitet. Die Daten müssen auch jederzeit schnell, sicher und in der geeigneten Form für den richtigen Personenkreis greifbar sein.

Analyse und Verbreitung der Informationen: Der Analysebereich des DAP ist die zentrale nationale Analysestelle. Alle nachrichtendienstlichen und kriminalpolizeilichen Informationen werden hier integral ausgewertet. In den vergangenen Jahren wurde der Bereich qualitativ und quantitativ ausgebaut. Es besteht eine enge Zusammenarbeit mit entsprechenden Stellen des Bundes und der Kantone.

Die Analyse im engeren Sinne umfasst das Zusammenführen von Informationen zu einem Gesamtbild. Hypothesen werden verifiziert oder falsifiziert und Schlussfolgerungen werden gezogen.

Analysen können beispielsweise als Bedrohungsanalyse oder als komparative Politikanalyse ausgestaltet werden oder aber Entwicklungen, Phänomene und Szenarien aufzeigen.

Zu den bekanntesten, weil öffentlichen Analyseprodukten des DAP gehören etwa die jährlich erscheinenden Berichte über die innere Sicherheit der Schweiz (BISS) oder der Extremismusbericht. Die Mehrzahl der Produkte ist jedoch vertraulicher Natur und behandelt ausgewählte Fragestellungen der inneren Sicherheit (wie z.B. die Abwehr gewaltextremistischer Ideologien auf juristischer, technischer und ideologischer Basis). Gleichzeitig zeigen diese Berichte auch auf, wo Wissenslücken bestehen, und steuern so die Planung der Informationsbeschaffung mit.

Ein weiteres Element der Gewährleistung der Sicherheit der Schweiz ist die ständige Verarbeitung und Verbreitung von aktuellen Lageinformationen. Das Bundeslagezentrum des DAP verbreitet zu diesem Zweck täglich aktuelle Lageberichte und Beurteilungen an über 300 Stellen im Bund und in den Kantonen.

Weiter führte die Erkenntnis über die Bedeutung des Internet und die Verletzlichkeit der schweizerischen Infrastruktur zur Schaffung der neuen Bereiche KOBIK (Koordinationsstelle Internetkriminalität von Bund und Kantonen) und MELANI (Melde- und Analysestelle Informationssicherung).

Informationsbeschaffung durch den DAP

Nach heutigem Recht bearbeitet der DAP Gefährdungen durch Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst, verbotenen Handel mit Waffen und radioaktiven Materialien sowie verbotenen Technologietransfer. Weiter unterstützt er die zuständigen Polizei- und Strafverfolgungsbehörden, indem er ihnen Erkenntnisse über das organisierte Verbrechen mitteilt, namentlich wenn solche bei der Zusammenarbeit mit ausländischen Sicherheitsbehörden anfallen.

Die im Rahmen der Prävention zulässigen Informationsbeschaffungsmittel sind in Artikel 14 Absatz 2 BWIS abschliessend aufgezählt. Danach können Personendaten beschafft werden durch:

a. Auswerten öffentlich zugänglicher Quellen;

b. Einholen von Auskünften;

c. Einsicht in amtliche Akten;

d. Entgegennahme und Auswerten von Meldungen;

e. Nachforschen nach der Identität oder dem Aufenthalt von Personen;

f. Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnungen;

g. Feststellen der Bewegungen und der Kontakte von Personen.

Der Gesetzgeber von 1997 hat dem DAP die Anwendung von Zwangsmitteln und das Beobachten in privaten Räumen, wie sie im Rahmen von eröffneten Strafverfahren zulässig sind, ausdrücklich untersagt. So ist heute beispielsweise die gesamte inländische Kommunikation (namentlich Post, Telefon, Telefax, E-Mail) der präventiven Informationsbeschaffung nicht zugänglich.

1.1.3 Weitere Aufgaben und Zuständigkeiten im Bereich der Sicherheit

Auslandnachrichtendienst

Der Strategische Nachrichtendienst (SND) im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) ist der Auslandnachrichtendienst der Schweiz.

Der SND als Auslandnachrichtendienst beschafft, gestützt auf Artikel 99 Absatz 1 des Militärgesetzes vom 3. Februar 1995[13] (MG), zuhanden der obersten politischen

13 SR **510.10**

und militärischen Führung, insbesondere für den Chef VBS, den Chef der Armee, den Sicherheitsausschuss des Bundesrates und die Lenkungsgruppe Sicherheit Informationen über das Ausland, die für die Sicherheit der Eidgenossenschaft bedeutsam sind, wertet diese aus und verbreitet sie. Er ist gemäss Artikel 99 Absatz 5 MG unmittelbar dem Chef VBS unterstellt. Der SND hat einen vom Sicherheitsausschuss des Bundesrates genehmigten Grundauftrag. Im Fokus der Beschaffungs- und Analysetätigkeit des SND stehen politische, wirtschaftliche, militärische und wissenschaftlich-technische Schwerpunktthemen. Darunter fallen auch Bedrohungen durch Terrorismus, organisierte Kriminalität und die Verbreitung von Massenvernichtungswaffen und deren Trägersystemen (Proliferation). Die Aufgaben des SND werden in der Nachrichtendienstverordnung VBS vom 26. September 2003[14] (VND) geregelt.

Polizei

Die hauptsächlich kantonaler Hoheit unterstehende Polizei sorgt für die öffentliche Sicherheit, Ruhe und Ordnung sowie die Bekämpfung der allgemeinen Kriminalität. Der Bund interveniert namentlich zur Bewältigung von Ereignissen, welche die Mittel und Möglichkeiten der Kantone übersteigen. Erfordert es die Lage, so kann er die Führung übernehmen.

Strafverfolgung

Bei der Strafverfolgung geht es darum, einen bereits vorhandenen Straftatverdacht und die damit zusammenhängende Frage der individuellen Tatschuld justizförmig zu klären.[15]

Abgrenzung der Aufgaben und Mittel des Inlandnachrichtendienstes von denjenigen der Strafverfolgungsbehörden

Zielsetzung der Informationsbeschaffung: Die Arbeit der Strafverfolgungsorgane bezweckt die einzelfallbezogene Klärung einer individuellen Verdachtslage. Die nachrichtendienstliche Informationsbeschaffung bezweckt hingegen, Gefährdungen oder Störungen der Sicherheit, gefährliche Absichten oder einschlägige Vorbereitungen frühzeitig zu erkennen. Werden solche aufgedeckt, so treffen die zuständigen Behörden von Bund und Kantonen die nötigen polizei- oder verwaltungsrechtlichen Abwehr- oder Beseitigungsmassnahmen.

Mittel der Informationsbeschaffung: Strafrechtliche Ermittlungen erfolgen im Rahmen eines förmlichen Ermittlungs- oder Strafverfahrens immer dann, wenn ein hinreichend gefestigter Verdacht auf eine konkrete Straftat aufgeklärt werden muss. Die Strafverfolgungsbehörden können im Zuge ihrer strafrechtlichen Ermittlungen nötigenfalls prozessuale Zwangsmittel (z.B. Vorladung, Zuführung, Festnahme, Polizeihaft, Untersuchungshaft, Sicherstellung und Verwahrung von Gegenständen, Beschlagnahme, Überwachung des Post- und Fernmeldeverkehrs, Untersuchung von Personen, erkennungsdienstliche Massnahmen, Observation, verdeckte Ermittlungen) anwenden. Aufgrund der geteilten Strafverfolgungskompetenz von Bund und

14 SR **510.291**

15 Für eine umfassende Gegenüberstellung von strafverfolgenden und präventiven Polizeiaufgaben s. Bericht des Bundesrates zum Postulat 05.3006 der sicherheitspolitischen Kommission des Ständerates vom 21. Februar 2005 «Effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen», Ziffer 3.2.4, Buchstabe a (BBl **2006** 5693), nachfolgend Bericht zum Postulat SiK genannt.

Kantonen gelangen neben den eidgenössischen Regelungen grundsätzlich 26 kantonale Polizei- und Strafverfahrensgesetze zur Anwendung; eine eidgenössische, einheitliche Strafprozessordnung befindet sich in parlamentarischer Beratung. Dem Inlandnachrichtendienst hat der Gesetzgeber die Anwendung vergleichbarer Mittel und das Beobachten in privaten Räumen untersagt. Die Frage, ob und wieweit dieses Verbot angesichts der aktuellen Gefährdungen durch Terrorismus und andere vergleichbare Gefahren weiter aufrechterhalten werden soll, ist Gegenstand der vorliegenden Teilrevision des BWIS.

Zuständigkeiten bei der Früherkennung von terroristisch und mafiös geprägter Schwerstkriminalität: Für die Früherkennung von Gefährdungen der inneren Sicherheit, die zusätzlich zur gegen Gesellschaft und Staat gerichteten Gewaltanwendung durch die politisch-ideologische Motivation ihrer Urheber charakterisiert sind, ist der DAP zuständig. Davon zu unterscheiden sind die nach wirtschaftlicher Bereicherung und gesellschaftlicher Anerkennung strebenden Syndikate «mafiösen» Zuschnitts; hier steht der kommerzielle Kontext im Vordergrund und die Früherkennung fällt in die kriminalpolizeiliche Zuständigkeitssphäre.[16]

Gerichtspolizeiliche Aufgaben: Von der nachrichtendienstlichen Früherkennung zu unterscheiden ist die Ermittlung von Straftaten sowie die Verfolgung von deren Urheber. Soweit die Gerichtsbarkeit des Bundes gegeben ist, ist für die Verfolgung von Straftaten mit organisiert kriminellem (mafiösem) Hintergrund ausschliesslich die Bundeskriminalpolizei (BKP) unter Leitung der Bundesanwaltschaft (BA) zuständig.[17]

Grenzen der Strafverfolgung

Der Zweck der Strafverfolgung setzt ihr gleichzeitig Grenzen. Die einzelfallweise Klärung konkreter Verdachtslagen ist nicht gemacht für die frühzeitige Erkennung von Gefährdungen oder übergeordneter Zusammenhänge. Die strafrechtlichen Tatbestände definieren strafbares Verhalten abschliessend und orientieren sich nicht an blossen Gefahrenlagen für ein Land oder seine Bevölkerung. Straftatbestände zur Verfolgung krimineller Organisationen, terroristischer Haupttaten oder terroristischer Zellen zielen über die generalpräventive Wirkung hinaus nicht primär auf die Verhinderung von Anschlägen. Auch strafbare Vorbereitungshandlungen orientieren sich nicht an Gefahrenlagen, sondern bestrafen individuell-konkrete Aktivitäten. Daraus ist ersichtlich, dass die Instrumente der Strafverfolgung weder konzipiert noch geeignet sind für die frühzeitige Erkennung von Gefahrenlagen und Risiken, von gefährlichen Individuen und Organisationen oder deren Strukturen. Dazu bedarf es vielmehr der nachrichtendienstlichen Arbeit, die sich an Gefahrenlagen und nicht an Straftaten orientiert.

16 Vgl. Bericht zum Postulat SiK, Ziffer 3.2.4, Buchstabe c
17 Vgl. Bericht zum Postulat SiK, Ziffer 3.2.4, Buchstabe d

1.1.4 Informationsaustausch und Zusammenarbeit mit anderen Behörden

Behördenorganisation im EJPD

Mit Blick auf die Ausdehnung der Bundesstrafgerichtsbarkeit auf kriminelle Organisationen hat der Bundesrat am 1. September 1999 die damalige Bundespolizei und den Sicherheitsdienst des Bundes von der BA in das damalige Bundesamt für Polizeiwesen (heute Bundesamt für Polizei, fedpol) überführt. Mit dem Entscheid, alle Polizeidienste des EJPD in diesem Bundesamt zu vereinigen, erfüllte der Bundesrat zum einen den Wunsch der Kantone nach einem einheitlichen polizeilichen Ansprechpartner auf Bundesebene. Zum anderen ist er der Forderung der PUK EJPD nachgekommen, den Bundesanwalt als öffentlichen Ankläger von seiner damaligen Stellung als oberstem Verantwortlichen der ehemaligen Bundespolizei zu entbinden, weil diese nebst ihren Aufgaben als gerichtliche Polizei des Bundes auch als Inlandnachrichtendienst amtete und mit präventiven Aufgaben betraut war[18].

Am 1. Januar 2001 sind dann mit dem Abschluss des Reorganisationsprojekts zur Bereinigung der Strukturen im Polizeibereich des Bundes die präventivpolizeilichen und die strafverfolgenden Aufgaben innerhalb des fedpol auch organisatorisch getrennt worden: Die ehemalige Abteilung «kriminalpolizeiliche Zentralstellendienste» und die «Bundespolizei» wurden durch die neu geschaffenen fedpol-Hauptabteilungen «BKP» und «DAP» abgelöst. Während die BKP als Gerichtspolizei heute die strafverfolgenden Aufgaben wahrnimmt, konzentriert sich die Zuständigkeit des DAP auf die nachrichtendienstliche Prävention.

Zusammenarbeit mit dem Auslandnachrichtendienst des VBS

Geht es bei den Gefährdungen um internationale Phänomene, die zum Aufgabengebiet sowohl des Inland- als auch des Auslandnachrichtendienstes gehören, arbeiten diese eng zusammen, heute vor allem im Rahmen von Plattformen in den Bereichen Terrorismus, organisierte Kriminalität und Proliferation.

Zusammenarbeit mit weiteren Stellen des VBS

Der DAP, der Militärische Nachrichtendienst (MND), der Luftwaffennachrichtendienst (LWND) und die übrigen Nachrichtenorgane der Armee sowie der militärischen Sicherheit unterstützen sich bei der Erfüllung ihrer Aufgaben. Die Unterstützung erfolgt namentlich durch Informationsaustausch, gegenseitige Beratung in Spezialgebieten sowie in der Ausbildung.

Kooperation zwischen dem DAP und den Strafverfolgungsorganen des Bundes

Thematische Überschneidung der Aufgabenfelder erfordert regelmässigen und raschen Informationsaustausch: DAP und BKP sind verpflichtet, die bei ihnen anfallenden Informationen, welche in den gesetzlichen Aufgabenbereich der anderen Stelle fallen, unverzüglich an diese weiterzugeben.[19]

Weitergabe von Informationen vom DAP an die BKP und die BA: Soweit beim DAP Informationen über organisiertes Verbrechen anfallen, hat er diese gemäss Artikel 2 Absatz 3 BWIS an die Strafverfolgungsorgane von Bund oder Kantonen weiterzu-

18 Bericht der Parlamentarischen Untersuchungskommission vom 22. November 1989, 89.006, Vorkommnisse im EJPD, BBl **1990** 637, Kap. VII Ziff. 1.
19 Vgl. Bericht zum Postulat SiK, Ziffer 3.2.5, Buchstabe a

leiten. Weiter ist er verpflichtet, strafverfolgungsrelevante Verdachtslagen unaufgefordert an inländische Strafverfolgungsbehörden weiterzugeben[20].

Weitergabe von Informationen von der BKP und der BA an den DAP: Als Korrelat dazu hat der Gesetzgeber BA und BKP zur Auskunft an den DAP verpflichtet[21]. Beide haben dem DAP unaufgefordert Meldung zu machen, wenn sie konkrete Gefährdungen der inneren oder der äusseren Sicherheit feststellen[22]. Über die Weitergabe von operativen Informationen hinaus teilt die BA dem DAP Urteile und Einstellungsbeschlüsse mit, wenn sie den Aufgabenbereich des BWIS betreffen.[23]

Informationsaustausch mittels Online-Verbindungen: DAP und BKP haben gegenseitige, beschränkte Zugriffe auf ihre Informationssysteme. Im Bundesgesetz über die polizeilichen Informationssysteme des Bundes ist zur Beschleunigung und Erleichterung der polizeilichen Amtshilfe die Schaffung eines nationalen Polizeiindexes vorgesehen.[24]

Verfahrensgarantien bei der Informationshilfe: Nebst dem Datenschutz haben Inlandnachrichtendienst und Strafverfolgungsbehörden auch überwiegenden öffentlichen Interessen Rechnung zu tragen, welche im konkreten Fall zu Einschränkungen oder zur gänzlichen Unterlassung der Informationshilfe führen können und auch die Weitergabe von Daten an dritte Stellen Restriktionen unterwerfen. So hat der DAP bei der Weitergabe nachrichtendienstlicher Erkenntnisse nebst dem generellen Vorbehalt überwiegender Interessen[25] den sog. Quellenschutz zu beachten. Während der Quellenschutz im Verkehr mit dem Ausland immer gilt[26], ist das Schutzbedürfnis der Inlandquellen in jedem einzelnen Fall gegen die entsprechenden Amts- oder Rechtshilfeinteressen abzuwägen. Die Weitergaben erfolgen deshalb in Form von ausgewerteten Berichten und nicht von Rohinformationen.

Die Weitergabe von Informationen kann auch seitens der BA und der BKP verweigert, eingeschränkt oder mit Auflagen versehen werden. Dies hat zu geschehen, wenn schutzwürdige Interessen einer betroffenen Person es verlangen[27] oder wenn wesentliche Strafverfolgungsinteressen es gebieten.[28]

Verkehr mit dem Ausland

Der DAP gewährleistet die Verbindungen zu ausländischen Sicherheitsbehörden, die Aufgaben im Sinne des BWIS erfüllen (Art. 8 BWIS), und vertritt die Schweiz in internationalen Gremien (Art. 6 der Verordnung vom 27. Juni 2001[29] über Massnahmen zur Wahrung der inneren Sicherheit [VWIS]). Die Bekämpfung des Terrorismus macht heute den überwiegenden Teil des internationalen nachrichtendienstlichen Informationsflusses aus.

20 Vgl. Art. 17 Abs. 1 BWIS und die Zusammenarbeitspflicht nach Art. 4 ZentG; vgl. Bericht zum Postulat SiK, Ziffer 3.2.5, Buchstabe b
21 Art. 13 Abs. 1 Bst. a BWIS
22 Art. 13 Abs. 2 BWIS
23 Vgl. Bericht zum Postulat SiK, Ziffer 3.2.5, Buchstabe c
24 Vgl. Bericht zum Postulat SiK, Ziffer 3.2.5, Buchstabe d
25 Art. 18 Abs. 5 VWIS
26 Vgl. Art. 17 Abs. 7 BWIS und Art. 20a VWIS
27 Vgl. Art. 102quater Abs. 2 i.V.m. Art. 27 Abs. 2 BStP und Art. 7 Abs. 2 der Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei
28 Vgl. Bericht zum Postulat SiK, Ziffer 3.2.5, Buchstabe e
29 SR **120.2**

Im Einzelnen pflegt der DAP eine kontinuierliche nachrichtendienstliche und polizeiliche Zusammenarbeit mit rund neunzig Partnerdiensten aus ausländischen Staaten und/oder internationalen Organisationen (z.B. UNO und EU)[30]. Der DAP ist Mitglied in vier informellen multilateralen Gremien: In der «Counter-Terrorism Group» (je ein Dienst aus jedem EU-Staat sowie aus Norwegen und der Schweiz), im «Club de Berne» (Dienste aus 22 europäischen Ländern), in der «Middle European Conference» (Dienste aus 17 Ländern, zudem 8 Länder mit Beobachterstatus, schwergewichtig im südosteuropäischen Raum) und in der «Police Working Group on Terrorism» (polizeiliche Anti-Terror-Behörden aus 26 Ländern). Als Voraussetzung für die Fortsetzung der nachrichtendienstlichen Zusammenarbeit mit dem «Situation Center» des Rates der EU ist der Abschluss eines Abkommen über die Sicherheitsverfahren für den Austausch von Verschlusssachen vorgesehen[31]. Auch nimmt der DAP im Rahmen der EAPC (Euro-Atlantic Partnership Council) für die Schweiz gegenüber der NATO die Aufgaben der Intelligence Liaison Unit (ILU) wahr.

Diese Zusammenarbeit entspricht bezüglich des Kreises der ausländischen Partnerdienste den aktuellen Bedürfnissen der Schweiz in allen Fachgebieten des BWIS.

Die nachrichtendienstliche Zusammenarbeit mit ausländischen Diensten ist informell. Sie beruht auf den Grundsätzen der Vertraulichkeit, der sog. Drittdienstregel und auf gegenseitigem Vertrauen. Informationen werden nach dem Grundsatz der gemeinsamen Interessen auf gleicher Ebene zur Verfügung gestellt, im Vertrauen darauf, dass einem der Partnerdienst seinerseits sicherheitsrelevante Informationen weiterleiten wird («do ut des», Geben und Nehmen). Eine Verpflichtung dazu besteht aber nicht.

30 Die internationale Kooperationsstrategie des DAP ist in einem vom Bundesrat im Juni 2005 genehmigten, vertraulich klassifizierten Dokument festgelegt.

31 Das Abkommen wurde vom Europäischen Rat am 24. Juni 2005, vom Bundesrat am 29. Juni 2005 genehmigt. Zur Zeit werden die technischen Detailbestimmungen mit der EU bereinigt.

1.1.5 Tabellarische Übersicht

Verdacht auf	
Gefährdung der Sicherheit der Schweiz durch Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst, Proliferation	**Konkrete Straftat oder strafbare Vorbereitung nach eidgenössischem oder kantonalem Strafrecht**
Prävention	*Repression*
Zuständigkeit	
Dienst für Analyse und Prävention kantonale Nachrichtendienste	Bundesanwaltschaft Bundeskriminalpolizei kantonale Strafverfolgungsbehörden
Tätigkeit	
nachrichtendienstliche Abklärungen und Informationsbeschaffung Analysetätigkeit im Bereich der inneren Sicherheit	justizförmige Klärung eines konkreten Straftatverdachts (gegebenenfalls unter Einsatz von strafprozessualen Zwangsmassnahmen)
Gegenstand	
alle sicherheitsgefährdenden Handlungen (unabhängig davon, ob sie einer Qualifikation als Straftat zugänglich sind oder nicht)	mit Strafe bedrohte Handlungen und für die Eröffnung eines Strafverfahrens hinreichender Tatverdacht
Zweck	
Abklärungen mit dem Ziel, Gewissheit über eine mögliche Gefährdung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz oder der Freiheitsrechte ihrer Bürgerinnen und Bürger zu erlangen Einleiten der notwendigen Massnahmen strategisch (dauerhafte Beobachtungstätigkeit)	Abklärungen mit dem Ziel, Gewissheit über die Begehung einer konkreten Straftat oder strafbaren Vorbereitungshandlung zu erlangen einzelfallbezogen (konkrete Straftat)
Resultat	
Bericht an politische Behörden politische oder administrative Massnahmen	Verfahrenserledigung durch Strafbehörden (Einstellung, Verurteilung, Freispruch) evtl. mit anschliessendem Strafvollzug
Informationsaustausch	
informeller Austausch mit ausländischen Nachrichten- und Sicherheitsdiensten	formeller Austausch mit ausländischen Justiz- und Polizeibehörden
Aufsicht	
Datenschutzorgane und politische Behörden	Datenschutzorgane und Strafjustizbehörden
Gesetzliche Grundlagen	
Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)	Zentralstellengesetz eidgenössisches und kantonales Strafrecht eidgenössisches und kantonales Strafverfahrensrecht

1.1.6 Sicherheitslage der Schweiz

Terrorismus

Sicherheitslage

Seit den Terroranschlägen von Madrid (2004; Anschläge auf Pendlerzüge) und London (2005; Anschläge auf U-Bahn und Busse) ist Westeuropa vom Ruhe- und Unterstützungsraum zu einem Operationsfeld des islamistischen Terrorismus geworden. Die allgemeinen Terrordrohungen richten sich gegen westliche Interessen gemeinhin, wozu aus fundamentalistisch-islamistischer Sicht z.B. auch die in der Schweiz angesiedelte UNO oder das IKRK gehören. Bezeichnend für die heutige Situation sind sehr kleine (und deshalb nur schwer infiltrierbare), autonom handelnde und nicht hierarchisch organisierte Zellen, die teils völlig unabhängig voneinander agieren und sich gegenüber Aussenstehenden abschotten. Der Einsatz moderner Kommunikationsmittel sowohl zur internen Kommunikation als auch zur Weiterverbreitung der Ideologie und damit Radikalisierung erfolgt fachkundig. Dies gilt besonders für internetbasierte Techniken. Hinzu kommt, dass sich die Täter und Täterinnen immer häufiger aus im Zielland geborenen und dort aufgewachsenen, ideologisch bisher unauffälligen Nachkommen ausländischer Immigrantinnen und Immigranten rekrutieren, die mit den jeweiligen Verhältnissen vor Ort (und ebenso deren Schwachstellen) bestens vertraut sind und den Eindruck einer guten Integration vermitteln. Rückschlüsse aus einschlägigen Strafverfahren im Inland und aus im benachbarten Ausland gewonnenen Erkenntnissen zeigen, dass die Schweiz von Personen ausgenutzt wird, die «Al-Qaida» unterstützen. Europäischen Sicherheitskräften gelang es bereits mehrmals, Planungen und Vorbereitungen terroristischer Gewaltakte im Vorfeld zu erkennen und zu vereiteln. So beispielsweise beim verhinderten Attentat auf den Weihnachtsmarkt in Strassburg (2000), bei den verhinderten Selbstmordanschlägen mit Flüssigsprengstoff auf Transatlantikflüge in England (2006) oder etwa bei vorzeitig aufgedeckten Plänen für Sprengstoffanschläge auf dänische Einrichtungen durch eine Dschihadisten-Gruppe (2006).

Die Sicherheitslage der Schweiz hat sich in den letzten Jahren im Zuge der oben geschilderten internationalen Entwicklung sukzessive verschlechtert und nachhaltig verschärft. Die Wahrscheinlichkeit von islamistisch motivierten Terroranschlägen hat sich auch in Westeuropa erhöht. Zwar blieb die Schweiz in der jüngeren Vergangenheit vor Terroranschlägen verschont. Doch kann sich diese Situation jederzeit ändern. Die heute für die Schweiz gültige Lage ist teilweise mit Konstellationen vergleichbar, bei denen es im Ausland zu ausgeführten oder versuchten Anschlägen kam. So gehört die Schweiz zur westeuropäischen Gefahrenzone, sie wird von Dschihadisten als sog. Kreuzfahrerstaat bezeichnet – was als legitimer Anschlagsgrund gilt –, und es gibt hier aktive, gewaltbereite und teilweise miteinander vernetzte islamistische Strukturen. Damit sind Potenziale für Terroranschläge grundsätzlich vorhanden. Wann oder ob sich die bestehenden Risiken realisieren, ist mit den heute vor allem auf öffentliche Quellen abzielenden Beschaffungsmitteln kaum vorhersehbar. In der Schweiz wurden aber auch Islamisten festgestellt, die sich als freiwillige Kämpfer am Dschihad im Irak beteiligen wollten. Dabei diente die Stadt Genf als Durchgangsort und zog Freiwillige aus der Westschweiz und dem benachbarten Frankreich an.

Nach heutiger Beurteilung ist die Schweiz nach wie vor kein primäres Ziel von islamistischem Terrorismus. Doch ist die allgemeine Gefahr für terroristische Aktionen in Europa gross, wovon auch die Schweiz – gleich wie andere westeuropäische

Länder – betroffen ist. In diesem Zusammenhang ist festzustellen, dass die Schweiz bei ihren heutigen Lagebeurteilungen von Informationen und den deutlich weiter gefassten Befugnissen der im Ausland mit der Aufklärung befassten Sicherheitsdienste profitiert. Eine durch mangelnde gesetzliche Grundlagen verursachte ungenügende Zusammenarbeit kann rasch dazu führen, dass das Ausland mit Informationen zugunsten der Schweiz viel restriktiver umgeht. Ungenügende Informationen können zu Fehleinschätzungen mit entsprechenden Folgen im Massnahmenbereich führen.

Lücken im präventiven Abwehrdispositiv

Ohne Eingriffe in die Privatsphäre lassen sich terroristische Strukturen der geschilderten Art weder rechtzeitig erkennen noch überwachen oder sonst wie genügend kontrollieren.

Nach geltendem Recht ist der Post- und Fernmeldeverkehr generell jeder Gefährdungsabklärung nach BWIS entzogen. Folge davon sind Lücken bei der Früherkennung und bei der internationalen Zusammenarbeit.

So schlossen etwa die italienischen Behörden aus der Fernmeldeüberwachung von Mailänder Islamistenkreisen, dass diese über Personen in der Schweiz die Ausbildung von Extremisten in Afghanistan organisieren und finanzieren. Die Voraussetzungen für die Einleitung eines Strafverfahrens gegen die in der Schweiz wohnhaften Personen waren nicht gegeben. Hingegen gelangten die italienischen Nachrichtendienste an den DAP mit dem Ersuchen um Abklärungen zum Umfeld der fraglichen Personen. Der DAP konnte die international üblichen, den privaten Bereich dieser Personen und ihres Umfeldes betreffenden Abklärungen nicht vornehmen. Dies weil u.a. kein Zugang zu Fernmeldedaten oder zu Informationen, die dem Postgeheimnis unterstehen, besteht. Da eine direkte Ansprache mit Rücksicht auf die italienischen Ermittlungen nicht in Frage kam, blieben die fraglichen Personen in der Schweiz unbehelligt (nach geltendem Recht ist auch der Einsatz technischer Überwachungsgeräte im privaten Bereich verboten). Fazit: Die nachrichtendienstliche Aufklärung von terroristischen oder extremistischen Netzwerken kann an der Schweizer Grenze enden.

Als weiteres Beispiel dienen drei im Dezember 2005 in Liechtenstein festgenommene türkische Staatsangehörige. Sie wurden beschuldigt, eine türkische Extremistengruppe, die für Selbstmordanschläge in Istanbul verantwortlich ist, finanziell und logistisch zu unterstützen. Im Zuge der Ermittlungen ergab sich eine rege Reisetätigkeit der Angeschuldigten in der Schweiz, insbesondere der mehrfache Besuch einer bestimmten Moschee. Von besonderem Interesse wären Detailkenntnisse über ihr hiesiges Beziehungsnetz gewesen, um allfällige Bezüge zu hiesigen Terrorgruppen oder deren Sympathisantinnen und Sympathisanten zu erkennen. Auch hier verhinderte der fehlende Zugang zu Fernmeldedaten entsprechende Abklärungen.

Europäische Inlandnachrichtendienste beziffern heute den Anteil von für die Terrorabwehr relevanten Erkenntnissen aus ihren präventiven Fernmeldeüberwachungen mit bis zu 80 Prozent.

Wo diese Kommunikation fehlt, müssen die Staatsschutzbehörden Nachrichten durch getarnte menschliche Kontakte zu den entsprechenden Gruppen und Personen zu gewinnen suchen, wozu heute fehlende Tarnidentitäten nötig sind.

Ein weiteres gravierendes Manko besteht im Bereich des Internets. Personen und Gruppierungen, welche die innere Sicherheit der Schweiz gefährden, nutzen zur

Propaganda und Weiterverbreitung ihres Gedankengutes sowie für den Informationsaustausch untereinander längst moderne EDV-Infrastrukturen, insbesondere das Internet.

Problematisch ist, dass beim Internet das Eindringen in passwortgeschützte Bereiche, in welchen beispielsweise djihadistische Propaganda verbreitet wird, zwar technisch möglich, aber – weil der Privatsphäre zurechenbar – verboten ist (Art. 143bis StGB, unbefugtes Eindringen in Datenverarbeitungssystem). Dies gilt auch dann, wenn mit einiger Wahrscheinlichkeit davon ausgegangen werden muss, dass ein System oder Datennetze genutzt werden, um für sich oder andere Daten zu speichern, welche die innere Sicherheit der Schweiz konkret gefährden können, und sich die Systeme im Ausland befinden. Die Aufklärung entsprechender Verdachtslagen ist ohne Zugang zur «Rohfassung» von verschlüsselt versandtem oder erhaltenem Mailverkehr oder zu über djihadistische Webseiten erreichbaren radikalen virtuellen Kontaktbereichen kaum möglich.

Mit dem generellen Ausschluss eines heute zentralen Informationsmediums von der präventiven Informationsbeschaffung wird ein gefährliches Wissensvakuum in Kauf genommen.

Fehlende Mittel lassen die Schweiz von ausländischen Informationen abhängig werden. So basieren die Erkenntnisse über die Radikalisierung von Teilen der bosnischen/slawischen Diasporagemeinde in der Schweiz durch radikale Koranauslegungen zur Hauptsache auf Informationen von ausländischen Partnerdiensten. Und ohne ausländisches Rechtshilfegesuch hätte die Schweiz keine Kenntnis über die hiesige Unterstützungsstruktur zugunsten einer algerischen Terrororganisation. Eine solche Abhängigkeit vom Ausland könnte sich fatal auswirken.

Verbotener Nachrichtendienst

Sicherheitslage

Ausländische Nachrichtendienste sind nach wie vor in der Schweiz selber oder gegen schweizerische Interessen im Ausland aktiv. Interesse besteht an politischen, wirtschaftlichen und militärischen Informationen.

Nach der Überzeugung des Bundesrates gilt es zu differenzieren zwischen politischem und militärischem Nachrichtendienst auf der einen und der Wirtschaftsspionage auf der anderen Seite. Bei der Wirtschaftsspionage sind in erster Linie die Unternehmen gefordert, geeignete Abwehrmassnahmen zu treffen.

Anders verhält es sich beim politischen und militärischen Nachrichtendienst. Hier sind adäquate staatliche Abwehrmassnahmen seit jeher unabdingbar.

Es fällt auf, dass seit dem Inkrafttreten des BWIS im Vergleich zu früher immer weniger mit Spionage befasste Personen im Einsatz enttarnt, Spionagestrukturen aufgeklärt und verbotener Nachrichtendienst nachgewiesen werden können. Der dadurch entstandene Eindruck, die Schweiz sei davon gar nicht mehr oder bloss noch geringfügig betroffen, kann indessen nicht zutreffen. Die von gewissen Ländern in der Schweiz stationierte Anzahl von Nachrichtendienstoffizieren belegt implizit einschlägige Aktivitäten. Gewisse ausländische Vertretungen in der Schweiz beschäftigen nachrichtendienstlich geschulte Mitarbeiterinnen und Mitarbeiter. Die «Agenten» gehören zum Botschaftspersonal, stehen unter dem Schutz der diplomatischen Immunität und sind dafür ausgebildet, unter Nutzung ihrer Tarnung auch nachrichtendienstlich Informationen zu beschaffen. Im Regelfall

besteht zu Beginn bloss eine nachrichtendienstliche Gefährdungsbeurteilung (z.B. aufgrund eines Hinweises eines befreundeten Nachrichtendienstes oder weil die Person Nachfolgerin einer als Angehörige eines fremden Nachrichtendienstes identifizierten Person ist). Hinzu kommen Abklärungen privater internationaler Ermittlungsbüros und Detekteien, die nicht selten in (getarntem) staatlichem Auftrag handeln.

Lücken im präventiven Abwehrdispositiv

Nach geltendem Recht sind nicht allgemein zugängliche Orte (z.B. Hotelzimmer) generell jeder Gefährdungsabklärung nach BWIS entzogen. Folge davon ist, dass Abklärungen über die innere Sicherheit der Schweiz grundsätzlich an der «Tür zum privaten Raum» enden. Dadurch können gewichtige Lücken im Abwehrdispositiv entstehen:

Da nachrichtendienstliche Beschaffungen, z.B. bei konspirativen Treffen, gerade unter besonderen Schutzvorkehren und oft im privaten Raum stattfinden, hat zwar die Schweizer Abwehrbehörde einen entsprechenden Gefährdungsverdacht. Sie kann aber, da sie nur Zugang zum öffentlichen Raum hat, die vermuteten Aktivitäten kaum aufklären und zu einem strafrechtlich relevanten Verdacht verdichten. Für strafrechtliche Ermittlungen besteht aber noch kein hinreichender Tatverdacht. Damit bleiben die zentralen Fragen ungeklärt: Welche Kontakte unterhält die Zielperson? Wer ist ihre Ansprechperson in der Schweiz? Was wird weshalb ausspioniert? Welche Methoden gelangen zum Einsatz? Besteht Raum für Gegenmassnahmen? usw.

Beim verbotenen Nachrichtendienst kann die Abwehrbehörde einschlägige Verdachtslagen ohne Zugang zum privaten Bereich kaum abklären, zumal die «Gegenspieler» speziell darauf geschult sind, die Schwächen der geltenden Gesetzgebung gezielt zu nutzen und ihre Aktivitäten professionell zu verheimlichen und zu vertuschen. Ohne Tarnidentitäten sind Gegenoperationen nur in Ausnahmefällen durchführbar; durch nicht durchführbare Gegenmassnahmen entgehen der Schweiz wichtige sicherheitsrelevante Erkenntnisse.

In Bezug auf das Ausforschen hiesiger Diasporagemeinden wird je länger je mehr festgestellt, dass Betroffene aus Angst vor ihnen oder ihren Angehörigen in Aussicht gestellten Nachteilen schweigen. Soll das Schweigen durchbrochen werden, sind nachrichtendienstliche Abklärungen im privaten Bereich unabdingbar (der Strafbehörde sind mangels genügendem Tatverdacht auch hier meistens die Hände gebunden).

Gewalttätiger Extremismus

Sicherheitslage

Als gewalttätiger Extremismus gelten Bestrebungen von Organisationen, deren Vertreter die Demokratie, die Menschenrechte oder den Rechtsstaat ablehnen und zum Erreichen ihrer Ziele Gewalttaten verüben, befürworten oder fördern (vgl. Art. 8 Abs. 1 Bst. c VWIS).

Extremistische Aktivitäten bergen ein Gewaltpotenzial in sich und können die innere Sicherheit eines Landes bedrohen. Deshalb gilt es, potenziell gewalttätige Aktivitäten extremistischer Organisationen frühzeitig zu erkennen und zu verhindern.

Sowohl die rechtsextreme als auch die linksextreme Szene der Schweiz bestehen aus vielen kleinen, zumeist miteinander vernetzten Gruppierungen. Man kann heute von einem Kern von insgesamt gegen 1200 Rechtsextremen in der Schweiz ausgehen; der linksextremen Szene sind rund 2000 Militante zuzurechnen. Auch ausländische extremistische Gruppen nutzen den grundrechtlich geschützten relativ grossen Handlungsspielraum in der Schweiz.

Lücken im präventiven Abwehrdispositiv

Nach Auffassung des Bundesrates kann der aktuellen Bedrohungslage mit der heutigen Rechtslage an sich genügend begegnet werden. Vorbehalten bleiben unerwünschte, die innere Sicherheit der Schweiz gefährdende Handlungsweisen bestimmter Personen oder Gruppierungen, die es zu unterbinden gilt. Zu denken ist etwa an Geldsammlungen gewaltextremistischer Organisationen in der Schweiz mit anschliessendem Geldtransfers ins Ausland, wo sich die Spuren des Geldes verlieren und keine Gewissheit über die weitere Verwendung der Spenden besteht, jedoch nicht ausgeschlossen werden kann, dass das Geld zur Finanzierung von Gewaltakten eingesetzt wird.

Verbotener Handel mit Waffen und radioaktiven Materialien sowie verbotener Technologietransfer (Proliferation)

Sicherheitslage

Unter Proliferation versteht man die Weiterverbreitung von nuklearen, chemischen und biologischen Waffen, ihrer Trägersysteme (z.B. Raketen) sowie zivil und militärisch verwendbarer Güter, die für die Herstellung notwendig sind. Auch der dazu notwendige Technologietransfer fällt darunter.

Die Schweiz ist Signatarstaat aller internationalen Abkommen, die den Handel mit Massenvernichtungswaffen untersagen, und aller Verträge zur Rüstungskontrolle.

Im Bereich der Proliferation sind regelmässig hochkomplexe Netzwerke tätig, die oft international agieren, weshalb in den einzelnen Ländern im Regelfall nur Puzzleteile sichtbar werden. Die entscheidenden Absprachen und Vorgänge erfolgen diskret im privaten Bereich. Nicht selten gehen mit solchen Geschäften auch sehr bedeutende Geldzahlungen einher, was die involvierten Personen zum Einhalten von noch grösseren Vorsichtsmassnahmen veranlasst. In einer ersten Phase liegen erfahrungsgemäss bloss vage Verdachtselemente für eine Sicherheitsgefährdung vor, so beispielsweise wenn eine einschlägig bekannte Person in die Schweiz einreist, ohne dass der konkrete Grund der Reise bekannt ist oder dieser zu Zweifeln oder zu Besorgnis Anlass gibt. Die Aufdeckung des auf Nukleartechnologie spezialisierten Transfernetzwerkes des «Vaters» der pakistanischen Atombombe, Dr. Abdul Qadeer Khan, zeigte nicht nur die komplexe und professionelle Struktur solcher Netzwerke auf, sondern auch, dass die Schweiz ohne weiteres in solche Machenschaften hineingezogen und ihre Infrastruktur gezielt für Beschaffungsaktivitäten benützt werden kann und wird. Dabei gilt das Interesse der Proliferationsstaaten allgemein der Schweizer Qualität und besonders einer Anzahl von Firmen aus dem Hochtechnologiesegment.

Als weitere Beispiele seien etwa auf die Bemühungen des Iran, Uran anzureichern, oder auf das Nuklearprogramm Nordkoreas hingewiesen. In Bezug auf die Bedrohung durch schmutzige Bomben (Bombe mit konventionellem Sprengkörper und einer unkonventionellen, z.B. radioaktiven Ummantelung) verstärkten die Schmugg-

ler gerade in Europa ihre Anstrengungen, sodass allein die Menge des von den Behörden in den Jahren 2003–2006 konfiszierten Materials derjenigen der vorangegangenen sieben Jahre entsprach.

Auch wird der DAP immer wieder von dritter Seite auf möglicherweise proliferationsrelevante Geschäfte von Schweizer Firmen aufmerksam gemacht. Die vorhandenen Indizien können jedoch wegen der ungenügenden Informationsbeschaffungsmöglichkeiten nicht zu einem für die Eröffnung eines Strafverfahrens hinreichenden Tatverdacht verdichtet werden. Im Ergebnis muss der DAP deshalb mit dem Vorliegen einer Straftat rechnen, kann indessen wenig dagegen unternehmen.

Lücken im präventiven Abwehrdispositiv

Gleich wie beim Terrorismus und verbotenen Nachrichtendienst sind auch im Proliferationsbereich die Abklärung entsprechender Verdachtslagen durch den Nachrichtendienst ohne Möglichkeit der Überwachung der Geheim- und Privatsphäre meistens wenig erfolgsversprechend.

So geht z.B. mit dem Kauf/Verkauf einer Werkzeugmaschine normalerweise keine Gefahr für die innere oder äussere Sicherheit einher. Anders kann es sich jedoch verhalten, wenn es sich um einen verdeckten Kauf für die Entwicklung von Massenvernichtungswaffen handelt (sog. Dual-Use-Güter). Auch hier sind mangels Zugang zum privaten Raum keine vertieften Abklärungen möglich, wenn zwar Hinweise für entsprechende Aktivitäten (z.B. aufgrund von Meldungen ausländischer Nachrichtendienste), nicht aber ein strafrechtlich relevanter Verdacht für verbotenes Tun besteht. Dies ist beispielsweise dann der Fall, wenn ausländische Nachrichtendienste die Schweiz auf die Einreise eines Geschäftsmannes hinweisen, der dem Umfeld eines unerwünschten ausländischen Nuklearprogramms zuzurechnen ist. Von besonderem Interesse wären hier seine Ansprech- und Geschäftspartner in der Schweiz bzw. der wahre Zweck der Reise. Die geltende Rechtslage lässt keine vertiefte Abklärung entsprechender Verdachtslagen zu.

Organisierte Kriminalität (OK)

Sicherheitslage

Das organisierte Verbrechen ist global und kann mittelfristig zu einer der grössten Bedrohungen für Gesellschaft, Staat und Wirtschaft werden. Die Einnistung in das normale Geschäftsleben durch Geldwäscherei, Korruption sowie den Aufkauf von Firmen und Immobilien bedroht die wirtschaftliche und gesellschaftliche Stabilität. Aber auch die Staaten selbst bzw. ihre Wirtschaftspolitik oder ihr Polizei- und Gerichtswesen sind oftmals Infiltrationsziele der OK. Schwerpunkte der zum Teil miteinander vernetzten kriminellen Gruppierungen sind Drogen-, Menschen- und Waffenhandel, Korruption, Erpressung sowie die damit verbundene Geldwäscherei. Anlass zur Sorge geben zudem mögliche Verbindungen zu terroristischen Gruppierungen.

Hoch entwickelte und international stark vernetzte Volkswirtschaften bieten kriminellen Organisationen viele Möglichkeiten zur Infiltration und zum Waschen von Gewinnen.

Vorhandenes Abwehrdispositiv

Nach Auffassung des Bundesrates wurde der aktuellen Bedrohungslage mit dem in den letzten Jahren erfolgten Ausbau von BA und BKP (sog. Effizienzvorlage) ausreichend Rechnung getragen.

1.1.7 Zusammenwirken von Nachrichtendienst und Strafverfolgung

Die Verfahren nach BWIS und StGB sind unterschiedlich

Sowohl nachrichtendienstliche Abklärungen (Prävention, vom lateinischen praevenire «zuvorkommen, verhüten»), als auch strafrechtliche Ermittlungen (Repression, vom lateinischen reprimere v. primere «drängen, drücken») werden durch konkrete Verdachtselemente ausgelöst. Für die Arbeit der Nachrichtendienste handelt es sich um einen Verdacht auf eine bedeutsame Gefährdung der Sicherheit der Schweiz oder ihrer Bevölkerung, für die Arbeit der Strafverfolgungsorgane um einen Verdacht auf eine konkrete Straftat.

Nachforschungen nach BWIS bezwecken die Klärung des Verdachts einer möglichen Gefährdung der Sicherheit der Schweiz oder ihrer Einwohnerinnen und Einwohner durch Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst oder durch Proliferation. Die Abklärungen können sowohl durch ein im Endeffekt strafloses, als auch strafbares Verhalten ausgelöst werden. Adressaten der Abklärungsresultate sind die politischen Entscheidungsträger, d.h. die Exekutivorgane von Bund und Kantonen, damit sie rechtzeitig nach ihrem massgebenden Recht eingreifen können, oder – bei Erhärtung eines strafrechtlichen Tatverdachts – die Strafverfolgungsorgane.

Anders verhält es sich bei der Strafverfolgung (Repression). Hier dient die Informationsbeschaffung der Klärung eines Straftatverdachts bzw. der individuellen Tatschuld und erfolgt beschränkt auf die jeweiligen Tatbestandsmerkmale. Die Strafverfolgungsorgane bringen die Resultate ihrer Ermittlungen in gerichtliche Verfahren ein und nicht vor politische Instanzen.

Die Abklärung von Gefahrenlagen nach BWIS unterscheidet sich also von den Ermittlungen bei strafrechtlich relevantem Handeln nach StGB, und zwar in Bezug auf das auslösende Ereignis (hier Verdacht auf Gefährdung der Sicherheit der Schweiz oder ihrer Einwohnerinnen und Einwohner, dort Verdacht auf Begehung einer konkreten Straftat), den Gegenstand der Abklärungen (hier Aufdecken von Strukturen und Netzwerken gemäss Aufgabenbereich BWIS, dort Nachweis tatbestandsmässigen Verhaltens gemäss StGB) und dem damit verfolgten Ziel (hier Entscheidungsgrundlage für durch die Exekutive zu ergreifende Massnahmen, dort Klärung eines Straftatverdachts bzw. einer individuellen Tatschuld).

Berührungspunkte bestehen dort, wo sich Abklärungen der Repression über strafbares Verhalten in einem konkreten Einzelfall mit präventiven Abklärungen über Gefährdungen der Sicherheit der Schweiz überschneiden, weil die unter Straftatverdacht stehende Person oder die mutmassliche Straftat gleichzeitig Gegenstand präventiver Interessen ist. Mit anderen Worten kann dieselbe Person oder Tat gemeinsame Abklärungen verursachen, dies jedoch unter unterschiedlichen Blickwinkeln: Hier Erhärtung des individuellen Verdachts auf eine konkrete Straftat, dort Teil einer umfassenden Abklärung zur Beurteilung einer Gefährdungslage der inneren

Sicherheit. Die jeweiligen Verfahren können sich deshalb teilweise ergänzen, aber nicht ersetzen.

Zur Verdeutlichung der unterschiedlichen Sichtweise sei auf das Beispiel einer ausländischen Organisation terroristischer Natur verwiesen. Einerseits ist diese dafür bekannt, mit nicht unzimperlichen Methoden bei Landsleuten in der Schweiz Spenden einzutreiben. Anderseits wird festgestellt, dass dieser Organisation zurechenbare Personen regelmässig mit grossen Bargeldbeträgen ins Ausland reisen. Aus strafrechtlicher Sicht kann kein strikter Beweis über die kriminelle Herkunft oder Verwendung des ausser Landes gebrachten Geldes erbracht werden. Damit mangelt es im Strafverfahren an einem notwendigen Tatbestandselement, was eine Verurteilung ausschliesst. Aus nachrichtendienstlicher Sicht hingegen ist häufig naheliegend, dass das fragliche Geld aus «Spenden» stammt und – auf welchen Wegen auch immer – der Finanzierung von Terroranschlägen oder des Krieges gegen das Heimatland dient. Da die Schweiz keine Förderung terroristischer Handlungen duldet, ist dieses Verhalten unerwünscht. Gestützt auf die Erkenntnisse des Nachrichtendienstes ist es Aufgabe der Exekutive, über das weitere Vorgehen, namentlich über geeignete Abwehrmassnahmen, zu befinden (z.B. Verbot von Geldsammlungen für bestimmte Gruppierungen oder Staatsangehörige).

Gefährdung der inneren Sicherheit der Schweiz durch strafloses und strafbares Tun

Auslösendes Element für Abklärungen nach BWIS sind Hinweise auf Verhaltensweisen oder Lageentwicklungen, die eine Gefährdung der inneren Sicherheit durch Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst oder Proliferation mit sich bringen.

Dabei kann die innere Sicherheit der Schweiz sowohl durch strafloses als auch durch strafbares Verhalten gefährdet werden. So drohte beispielsweise das damalige irakische Regime unter Saddam Hussein für den Fall eines Kriegsausbruches mit weltweiten, aus dem Schutz diplomatischer Missionen Iraks begangenen Terroranschlägen. Für die Schweiz lagen keine konkreten Hinweise auf die Vorbereitung strafbarer Handlungen vor, die in einem Strafverfahren hätten geklärt werden können. Trotzdem lag es in der Verantwortung der Schweizer Regierung, die Situation zu beurteilen und Massnahmen zur Minimierung des Risikos von Anschlägen in der Schweiz oder von ihrem Gebiet ausgehend zu treffen. Hierzu waren und sind nachrichtendienstliche Erkenntnisse notwendig.

Für die sicherheitspolitische Beurteilung einer Gefährdungslage ist demnach weder die Straflosigkeit noch die mutmassliche Strafbarkeit einer bestimmten Verhaltensweise das allein ausschlaggebende Kriterium.

Fehlende nachrichtendienstliche Mittel verhindern bessere Unterstützung der Strafverfolgungsbehörden

Voraussetzung für jedes Tätigwerden von Strafverfolgungsbehörden ist ein Anfangstatverdacht. Auf Bundesebene z.B. wird für die Aufnahme von Ermittlungshandlungen das Vorliegen eines «hinreichenden» Tatverdachts verlangt (vgl. Art. 101 Abs. 1 BStP; ebenso Art. 194 Abs. 1 Ziff. 2 E-StPO).

In der Praxis ergeben nachrichtendienstliche Abklärungen von Gefährdungen der inneren Sicherheit nicht selten Indizien für das Vorliegen oder Planen möglicher Straftaten, ohne dass hinsichtlich möglichen Täterkreises oder Konkretisierungsgra-

des der Vorbereitungen bereits ein strafrechtlich relevanter Tatverdacht begründet ist.

Folge davon ist, dass der Nachrichtendienst zwar mit dem Vorliegen einer Straftat rechnen muss, indessen über kein Instrumentarium verfügt, die ihm bekannten Indizien zu einem genügenden Tatverdacht zu verdichten. Die Strafbehörden verfügen ihrerseits zwar über ein genügendes Instrumentarium, dürfen dieses bei derartigen Konstellationen indessen mangels genügenden Tatverdachts nicht zum Einsatz bringen.

Sollen weder solche Lücken in Kauf genommen noch Strafverfahren ohne hinreichenden Tatverdacht eröffnet werden, sind für die nachrichtendienstliche Früherkennung vertiefte Abklärungsmöglichkeiten zu schaffen.

1.1.8 Beurteilung der Risikofelder

Ein gewisses Sicherheitsrisiko

Das BWIS regelt den präventiven Staatsschutz in der Schweiz. Es ist massgeblich von der sog. «Fichenaffäre» geprägt und misst Fragen des Datenschutzes in der nachrichtendienstlichen Tätigkeit überwiegendes Gewicht bei. Auf Informationsbeschaffungsmassnahmen, welche die Privatsphäre tangieren, wird weitgehend verzichtet. Das Schwergewicht liegt auf der Begrenzung des Staatsschutzes und weniger auf seiner Schutzfunktion zugunsten der Öffentlichkeit. Diese Optik wurde denn auch ausdrücklich in der damaligen Botschaft festgehalten:

«Das Gesetz sieht die Informationsbearbeitung im Vorfeld der Strafverfolgung nur bei unbedingter Notwendigkeit vor. Der Bund nimmt damit ein gewisses Sicherheitsrisiko in Kauf, …» (Botschaft zum BWIS, BBl *1994* II 1129).

Mit der verschärften Bedrohungslage ist auch das seinerzeit in Kauf genommene Sicherheitsrisiko gewachsen. Die für eine Früherkennung notwendigen Informationsbedürfnisse können seit längerer Zeit nicht mehr ausreichend befriedigt werden; der Bundesrat wies bereits in der am 26. Juni 2002 zuhanden des Parlamentes verabschiedeten «Lage- und Gefährdungsanalyse Schweiz nach den Terroranschlägen vom 11. September 2001» auf die Schwachstellen bei der Bekämpfung terroristischer Gefahren hin.

Erkannte Lücken im präventiven Abwehrdispositiv

Abklärungen nach BWIS sollen Gefährdungen der Sicherheit der Schweiz oder ihrer Einwohner frühzeitig erkennen, damit solche wenn möglich verhindert werden können. Dabei mangelt es der Früherkennung an einem Instrumentarium, das erlaubt, bei begründetem Anlass vertiefte Abklärungen auch im privaten Bereich tätigen zu können.

Werden Gefährdungslagen nicht oder zu spät erkannt, sind Präventionsmassnahmen nur verspätet oder gar nicht mehr möglich.

Bei der Zusammenarbeit mit dem Ausland führt ein allzu grosses Gefälle in den jeweiligen nationalen Sicherheitsinstrumentarien zu unterschiedlichen Standards. Ab einem gewissen Mass wird dadurch die eigene Glaubwürdigkeit in Frage stellt. So gelangte etwa das United States Department of State im «Country Reports on Terrorism 2006» in Bezug auf die Schweiz u.a. zu folgendem Schluss: «… however,

law and practice continued to limit the scope of intelligence sharing and joint investigations …» (S. 75). Es besteht die Gefahr, dass selbst befreundete Dienste zur Wahrung ihrer Interessen auf Schweizer Gebiet operationell werden, was sich in etlichen Fällen bereits bestätigte.

Keine strategischen Überwachungen möglich

Staatsschutzrelevanten Gefährdungen terroristischen Zuschnitts liegen in der Regel politisch-ideologische Motivationen zu Grunde. Radikal-fundamentalistische Überzeugungen sind im Regelfall einer Deeskalation nicht zugänglich, da sie sich gegenüber jeder Argumentation verschliessen und von unbestimmter Dauer sind.

Erfahrungsgemäss können sich aus derartigen Risikolagen jederzeit konkrete Aktionen mit Gefährdungen der Sicherheit der Schweiz ergeben. Oft sind die dabei wirksamen Faktoren unwägbar; in vielen Fällen haben sich extremistische Ansichten zu Gewaltextremismus gewandelt und in einzelnen Fällen kam es sogar zu Terroranschlägen. Ein solcher Anschlag kann auch in der Schweiz nicht ausgeschlossen werden; Potenziale sind vorhanden und entsprechende Absichten wurden geäussert.

So wurden beispielsweise bei einem Schweizer mit terrorismusfreundlicher Gesinnung Chemikalien sichergestellt, welche die Herstellung von mehreren Kilo Sprengstoff erlaubt hätte. Nachdem das Strafverfahren mangels gerichtsverwertbarer Beweise eingestellt werden musste, lassen verschiedene Hinweise auf eine weitere Radikalisierung schliessen (ohne dass die Schwelle zur strafbaren Vorbereitungshandlung bereits überschritten worden ist, weshalb keine Strafverfolgung erfolgen kann).

Ein ungehindertes Gewährenlassen von solchen Personen oder Gruppierungen ist ein Risiko, das die Schweiz nicht in Kauf nehmen darf. Es wird sich immer häufiger die Frage nach der langfristigen Überwachung von Personen stellen, die z.B. wegen terroristischer Aktivitäten strafrechtlich verurteilt wurden, nun aber ihre Strafe verbüsst haben und wieder in Freiheit sind, oder die aus Mangel an Beweisen für konkrete strafbare Handlungen freigesprochen wurden, aber erkennbar weiterhin ihr gewaltorientiertes Gedankengut pflegen und Gewaltakte nicht ausschliessen.

Es braucht deshalb Rechtsgrundlagen für strategische, auf längere Wirkung gerichtete, aber gezielte, auf das Notwendige beschränkte und gerichtlich und politisch kontrollierte nachrichtendienstliche Überwachung im Inland.

Verbot von sicherheitsrelevanten Tätigkeiten

Zum Schutz der inneren Sicherheit sollen gewisse Tätigkeiten unterbunden werden können. Namentlich die Förderung von terroristischen oder gewaltextremistischen Umtrieben soll verboten werden können, wenn sie die innere oder äussere Sicherheit der Schweiz konkret gefährden (z.B. Verbot für Geldsammlungen in der Schweiz zur Finanzierung eines Krieges oder einer kriegsführenden Partei im Ausland).

Solche Verbote sind nach heutigem Recht bereits beschränkt und in ausserordentlichen Gefahrensituationen möglich. Sie stützen sich auf Artikel 184 Absatz 3 und Artikel 185 Absatz 3 BV. Allerdings müssen sie befristet werden und eine mehrmalige oder unbefristete Verlängerung ist nicht möglich, weil dies der Verfassung widerspräche. Deshalb soll eine gesetzliche Grundlage geschaffen und die Entscheidkompetenz in Anwendungsfällen nach BWIS an das EJPD delegiert werden. Gleichzeitig wird damit auch der Rechtsschutz erhöht.

Eine abschliessende Auflistung der mit einem Verbot zu erfassenden Tätigkeiten ist nicht sachgerecht, da sich die dem Einzelfall anzupassenden Details eines Verbotes abstrakt nicht präzise festlegen lassen. Zudem erfolgte eine Annäherung an das Strafrecht und die Regierung könnte ihre Verantwortung für die Wahrung der inneren Sicherheit nur ungenügend wahrnehmen. Entscheidend ist, dass die betroffene Person oder Organisation nach der Verhängung eines Verbotes ihre Pflichten kennt und ihre Rechte wahrnehmen kann. Dies lässt sich am besten erreichen, wenn die im jeweiligen Einzelfall einzuhaltenden Verpflichtungen dem zu beurteilenden Sachverhalt individuell angepasst werden. Mit der hier vorgeschlagenen Vorgehensweise kann diesem Erfordernis bestmöglich Rechnung getragen werden.

Dieses Vorgehen erlaubt einer Verbesserung der präventiven Gefahrenabwehr, indem die gesetzliche Möglichkeit geschaffen wird, rasch und unmittelbar auf das Verhalten von Personen oder Gruppierungen reagieren zu können.

1.2 Untersuchte Lösungsmöglichkeiten

1.2.1 Konsequentes Ausschöpfen bestehender Möglichkeiten im Bereich des Strafrechts und des präventiven Staatsschutzes

Die heutigen gesetzlichen Kompetenzen, soweit sie politisch beeinflusst werden können, werden bereits weitestgehend ausgeschöpft. Die zur Schliessung der Sicherheitslücken erforderlichen Informationen für die politische und exekutive Ebene lassen sich aber selbst mit einer extensiven Auslegung und Anwendung des heutigen Rechts nicht beschaffen. Eine politische Instrumentalisierung des Strafrechts zu präventiven Zwecken ist aber abzulehnen. Strafverfahren dürfen nicht zur Erfüllung von Informationsbedürfnissen der politischen Führung oder zur nachrichtendienstlichen Informationsbeschaffung durchgeführt werden, etwa indem die Anforderungen für deren Eröffnung herabgesetzt, oder indem sie auf Weisung der sicherheitspolitischen Instanzen eröffnet werden. Die Unabhängigkeit der Strafverfolgung muss gewahrt bleiben, auch wenn diese punktuell wichtige Erkenntnisse für die Wahrung der inneren Sicherheit liefern kann. Die bestehenden Lücken bei der Früherkennung und Lagebeurteilung können durch diese Erkenntnisse nicht geschlossen werden.

1.2.2 Verbesserung des Informationsflusses und der Koordination zwischen Repression und Prävention

Die Zusammenarbeit zwischen den Strafverfolgungsbehörden des Bundes und dem Inlandnachrichtendienst bildete bereits Gegenstand vertiefter Prüfung durch den Bundesrat.[32] Dabei erkannte der Bundesrat keinen Bedarf für neue gesetzliche Massnahmen in diesem Bereich.

32 Bericht zum Postulat SiK

1.2.3 Ausbau des formellen und materiellen Strafrechts

Der Bundesrat prüfte im Rahmen seines Berichtes zum Postulat SiK auch, ob und inwieweit mit Blick auf eine effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen gesetzgeberischer Handlungsbedarf besteht, und gelangte zum Schluss, im heutigen Zeitpunkt seien gesetzgeberische Massnahmen verfrüht. Vielmehr sei es angezeigt, zunächst die Erkenntnisse aus hängigen oder anstehenden gerichtlichen Beurteilungen sowie die Ergebnisse der parlamentarischen Beratung zum vorliegenden Revisionsentwurf BWIS abzuwarten.

1.2.4 Ausbau des präventiven Staatsschutzes

Die festgestellten Lücken beschlagen die präventive Gefahrenerkennung und Gefahrenabwehr und damit in erster Linie den präventiven Staatsschutz. Da das BWIS die Aufgaben und Mittel des präventiven Staatsschutzes regelt, sind Verbesserungen auch dort zu regeln. Im Übrigen kann auch hier auf ein bewährtes System mit bestehenden Strukturen zurückgegriffen werden.

Überdies sprechen folgende weitere Punkte für einen Ausbau des BWIS:

- Die Prävention ist ein von der Sicherheitspolitik gesteuertes Instrument: Es ist die Politik bzw. die Exekutive, die ihre Informationsbedürfnisse im Rahmen des Gesetzes definiert und entsprechende Aufträge erteilt. Es ist die Politik bzw. die Exekutive, die in die Lage versetzt werden soll, sicherheitspolitische Gefahren frühzeitig zu erkennen und in die politische Beurteilung mit einzubeziehen. Und schliesslich ist es wiederum die Politik bzw. die Exekutive, die u.a. gestützt auf die Erkenntnisse der eidgenössischen und kantonalen Sicherheitsbehörden ihre sicherheitspolitischen Entscheide trifft und dafür die politische Verantwortung trägt. Es ist deshalb sachgerecht, die festgestellten Lücken im präventiven Abwehrdispositiv im Rahmen des unter der Kontrolle und Aufsicht der Politik stehenden BWIS zu schliessen.
- Nach heutigem Recht ist nur eine beschränkte Früherkennung und Lagebeurteilung möglich, weil mit dem heutigen Instrumentarium weder genügende Informationen über Vorkommnisse im eigenen Land erhoben werden können noch eine wirksame strategische Beobachtung erkannter Gefahrenherde möglich ist.
- Für die Bekämpfung von Terrorismus und vergleichbaren Gefahren müssen alle grundrechtskonform einsetzbaren Mittel angewendet werden, d.h. sowohl das repressive als auch das präventive Instrumentarium. Für die Früherkennung und Gefahrenabwehr, d.h. die Verhinderung von Terror- oder ähnlichen Anschlägen ist vorab die Prävention und damit die Arbeit der Nachrichtendienste gefordert.
- Die Bekämpfung terroristischer Handlungen muss besonders früh einsetzen, um diese bereits im Stadium der Planung und Vorbereitung zu erkennen und zu vereiteln. Dazu sind Massnahmen zur wirksamen Beobachtung gefährlicher Personen und Strukturen sowie eine optimale internationale Zusammenarbeit notwendig. Aber selbst nach einem erfolgten Terroranschlag sind – wie ausländische Beispiele belegen – für eine rasche Ermitt-

lung der Täterschaft oft nachrichtendienstliche Erkenntnisse von entscheidender Bedeutung.

- Grosse Unterschiede bei den jeweiligen nationalen Sicherheitsinstrumentarien führen zu unterschiedlichen Standards. Die Annäherung einiger nachrichtendienstlicher Befugnisse an jene der meisten Nachbarländer soll verhindern, dass die Schweiz zu einem Raum geringerer Sicherheit wird.
- Mit einem Ausbau des BWIS wird die internationale Zusammenarbeit nachhaltig gestärkt.
- Von einem Ausbau des BWIS werden die strafprozessualen Grundsätze, wonach strafrechtlich motivierte Ermittlungen eines hinreichenden Tatverdachts bedürfen und strafwürdiges Verhalten für die Rechtsunterworfenen präzise beschrieben sein muss, nicht unterlaufen.
- Der Ausbau der Prävention ermöglicht dauerhafte und vertiefte Erkenntnisse über sicherheitsgefährdende Bereiche, die letztlich auch schwerstkriminell sind. Diese Erkenntnisse («intelligence») können die punktuell agierenden Strafverfolgungsorgane wirkungsvoll unterstützen und ermöglichen diesen den zielgerichteten Einsatz ihrer Ressourcen.
- Durch gezielte nachrichtendienstliche Abklärungen und entsprechende frühzeitige Massnahmen können gravierende Straftaten verhindert, auf die aufwendige Durchführung von Strafverfahren verzichtet und dadurch die Strafverfolgungsbehörden wirksam entlastet werden.

1.2.5 Weitere Gesetzgebungsprojekte

Die Gesetzgebung im Bereich der Polizei und Strafverfolgung befindet sich in einem ständigen Anpassungs- und Erneuerungsprozess. Zur Zeit werden zahlreiche internationalen Vereinbarungen, Gesetze und Verordnungen neu geschaffen oder revidiert. Zwischen diesen Projekten und dem vorliegenden Gesetzgebungspaket bestehen keine direkten relevanten Bezüge.

In diesem Zusammenhang sei namentlich auf die laufende Bereinigung des Polizeirechts des Bundes (vgl. 06.3285, Interpellation Banga, Innere Sicherheit. Verfassungsrechtliche Ordnung und Kompetenzaufteilung zwischen Bund und Kantonen im Bereich des Polizeirechts) sowie auf die Gesetzgebungsarbeiten zu einem Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) und zum Bundesgesetz über die Anwendung von Zwang im Ausländerrecht und beim Transport von Personen im Auftrag der Bundesbehörden (Zwangsanwendungsgesetz, ZAG) beziehungsweise zur Schaffung einer neuen Verfassungsbestimmung «Hooliganismus» verwiesen.

Die vorliegende Revision bezweckt in erster Linie die Verbesserung der präventiven Informationsbeschaffung für die sicherheitspolitische Lagebeurteilung und daraus abgeleiteter Massnahmen im Interesse der inneren und äusseren Sicherheit des Landes.

Die Anpassung der Rechtsgrundlagen für den strategischen Nachrichtendienst im VBS wird separat geprüft. Für den Auslandnachrichtendienst sind die Anforderungen an den rechtlichen Rahmen wesentlich anders als für den polizeilich arbeitenden

Inlandnachrichtendienst, weshalb in dieser Revision nur ein dringender Teilbereich abgedeckt wird, der beide Dienste betrifft (strategische Funkaufklärung).

1.3 Die beantragte Neuregelung

Die Gesetzesrevision zielt auf die Umsetzung der Folgerungen, die sich aus der am 26. Juni 2002 zuhanden des Parlamentes verabschiedeten «Lage- und Gefährdungsanalyse Schweiz nach den Terroranschlägen vom 11. September 2001» und aus den parlamentarischen Vorstössen nach dem 11. September 2001 ergeben.

Um dieses Ziel zu erreichen, soll einerseits das bei der Beschaffung von Informationen zum Einsatz gelangende nachrichtendienstliche Instrumentarium wirksamer gestaltet und dem europäischen Standard angenähert werden. Beschränkt auf die Abwehr von Terrorismus, verbotenem politischen oder militärischem Nachrichtendienst und verbotenem Handel mit Proliferationsgütern (Weiterverbreitung von Massenvernichtungswaffen) sollen die Behörden und Verwaltungseinheiten des Bundes und der Kantone in konkreten Fällen zur umfassenden Auskunftserteilung verpflichtet werden. Unter denselben Voraussetzungen sollen auch gewerbliche Transporteure auskunftspflichtig werden, soweit bei ihnen bereits vorhandene Daten benötigt werden. Weiter sollen unter strengen Voraussetzungen besondere Mittel zur Informationsbeschaffung eingesetzt werden können. Wiederum beschränkt auf die Bereiche Terrorismus, verbotener politischer oder militärischer Nachrichtendienst und Proliferation soll bei hinreichend konkreter Gefährdung der inneren Sicherheit das Überwachen des Post- und Fernmeldeverkehrs, das Beobachten an nicht allgemein zugänglichen Orten, auch mittels technischem Überwachungsgerät, sowie das geheime Durchsuchen von EDV-Systemen ermöglicht werden.

Der Einsatz von besonderen Mitteln zur Informationsbeschaffung wird einer doppelten Kontrolle unterstellt: Auf Antrag des Bundesamts für Polizei entscheidet das Bundesverwaltungsgericht über die Rechtmässigkeit der Massnahmen (Genehmigungsverfahren). Im Rahmen dieses Entscheides prüfen sodann die Vorsteher oder die Vorsteherinnen des EJPD und des VBS den Antrag nach staatspolitischen Gesichtspunkten und entscheiden im Einvernehmen über die Massnahme (Anordnungsverfahren). Verneint das Bundesverwaltungsgericht die Rechtmässigkeit der Massnahme, entfällt das Anordnungsverfahren.

Die Überwachung mit besonderen Mitteln muss der betroffenen Person in einer späteren Phase mitgeteilt werden; vorbehalten bleiben im Einzelfall höher zu gewichtende öffentliche Interessen sowie Interessen zum Schutz von Dritten. Über Ausnahmen von der Mitteilungspflicht entscheidet das Bundesverwaltungsgericht bzw. der Departementsvorsteher oder die Departementsvorsteherin EJPD bzw. VBS im zur Anordnung besonderer Informationsbeschaffungsmittel analogen Verfahren (Genehmigungs- bzw. Anordnungsverfahren).

Der Vorsteher oder die Vorsteherin des EJPD soll die Kompetenz erhalten, einer Person, Organisation oder Gruppierung bestimmte Tätigkeiten zu verbieten (z.B. Geldsammlung), soweit die Tätigkeiten mittelbar oder unmittelbar terroristische oder gewaltextremistische Umtriebe propagieren, unterstützen oder in anderer Weise fördern und so die innere oder äussere Sicherheit der Schweiz konkret gefährden. Bisher war dies nur dem Bundesrat, gestützt auf seine besonderen Verfassungskompetenzen, für beschränkte Zeit möglich. Im Gegenzug erhalten betroffene Personen

einen Rechtsmittelweg, was gegen verfassungsunmittelbare Verfügungen und Verordnungen des Bundesrates im Prinzip nicht möglich ist.

Weiter soll die Möglichkeit der Inanspruchnahme von Informantinnen und Informanten und die Natur der ihnen gewährten finanziellen Entschädigung (weder AHV- noch steuerpflichtiges Einkommen) formellgesetzlich geregelt und daneben die Möglichkeit geschaffen werden, solche Personen bei Notwendigkeit zu schützen. Um bei der Informationsbeschaffung den Schutz von Informantinnen und Informanten und Mitarbeitenden des DAP sicherzustellen, wird die für den strategischen Nachrichtendienst bereits bestehende Möglichkeit zur Legendierung (Tarnidentität) auch für den Inlandnachrichtendienst geschaffen. Schliesslich wird die (seit langem bewährte) Lagedarstellung durch das Bundeslagezentrum gesetzlich geregelt und mit einer Ergänzung im Bereich der Personensicherheitsprüfungen (sog. «Clearing») wird sichergestellt, dass Schweizerinnen und Schweizer wie auch hier wohnhafte ausländische Personen auch künftig die Möglichkeit haben, an klassifizierten Projekten des Auslandes mitzuarbeiten.

1.4 Begründung und Bewertung der vorgeschlagenen Lösung

Die Sicherheits- und Gefahrenlage der Schweiz hat sich in den letzten Jahren vor allem bedingt durch internationale Entwicklungen sukzessive verschlechtert. Namentlich mit der erhöhten Wahrscheinlichkeit von islamistisch motivierten Terroranschlägen wurde die Lage langsam aber stetig unwägbarer. Mit den heute für die nachrichtendienstliche Informationsbeschaffung zulässigen Mitteln ist keine der veränderten Gefahrenlage angepasste Früherkennung mehr möglich. Es besteht ein gefährliches Erkenntnisvakuum. Werden Gefährdungslagen nicht oder zu spät erkannt, kommt es (soweit beispielsweise nach einem Terroranschlag dann überhaupt noch möglich) zu verzögerten Präventionsmassnahmen und damit zu einer Gefährdung der Bevölkerung.

Für rechtzeitige Präventionsmassnahmen ist eine bessere Informationsbeschaffung notwendig, wofür in einzelnen Fällen gezielte Eingriffe in die Privatsphäre erforderlich sind. Entsprechende Grundrechtseingriffe sollen bei konkreten Hinweisen auf wesentliche Gefährdungen der inneren Sicherheit der Schweiz, nach richterlicher Kontrolle und unter politischer Verantwortung des Departementsvorstehers EJPD ermöglicht werden. Mit anderen Worten soll das geltende, vor einem anderen Gefährdungshintergrund beschlossene generelle Verbot von Eingriffen in die Privatsphäre durch ein Verbot mit Erlaubnisvorbehalt ersetzt werden. Dabei geht es um wenige – aber potenziell wichtige – Fälle pro Jahr.

Im Kampf gegen Terrorismus und andere vergleichbare Gefahren sollen alle verfügbaren Mittel zum Einsatz gelangen, d.h. sowohl das repressive als auch das präventive Instrumentarium. Für die Früherkennung und Gefahrenabwehr, d.h. die Verhinderung von Terroranschlägen oder anderen vergleichbaren Gefahren, ist in erster Linie die Prävention und damit die Arbeit der Nachrichtendienste gefordert.

1.4.1 Ergebnis des Vernehmlassungsverfahrens

Alle Kantone mit Ausnahme von Bern stimmen der Vorlage ausdrücklich oder dem Grundsatze nach zu, teilweise mit Vorbehalten und etliche mit dem Wunsch nach ausführlicherer Begründung der Notwendigkeit der Revision.

Zustimmung signalisieren die Evangelische Volkspartei und die Liberale Partei. Grundsätzlich positiv steht die Christlichdemokratische Volkspartei der Vorlage gegenüber. Die Freisinnig-Demokratische Partei unterstützt die Stossrichtung der Gesetzesrevision, verlangt jedoch Anpassungen und thematisiert Klärungsbedarf bei der Führung und Koordination der Nachrichtendienste. Abgelehnt wird die Vorlage von der Schweizerischen Volkspartei (Neutralität anstelle von präventiven Überwachungsmassnahmen), der Sozialdemokratischen Partei (Mittel der Strafverfolgung ausreichend und gegebenenfalls ausbaubar), und der Grünen Partei (keine «Vorfeld-ermittlungen» ohne konkreten Straftatverdacht). Gemäss Bundesgericht wird sich die Verhältnismässigkeit der Massnahmen in der konkreten behördlichen Praxis und den gerichtlichen Entscheidungen ermessen lassen. Daraus lässt sich schliessen, dass das Bundesgericht die Massnahmen als grundrechtskonform anwendbar erachtet.

Der Schweizerische Gemeindeverband und der Schweizerische Städteverband beurteilen die Vorlage zustimmend. Economiesuisse unterstützt eine Anpassung des Instrumentariums an die gewandelte Bedrohungslage, fordert jedoch eine Stärkung des Rechtsschutzes. Swiss Banking hat Verständnis für die vorgeschlagenen Massnahmen. Der Schweizerische Gewerkschaftsbund lehnt die Vorlage ab (heutige Gesetzgebung genüge).

Viele Stellungnahmen fielen diametral entgegengesetzt aus. Ablehnend äusserten sich Organisationen wie Amnesty International (Strafrecht ausreichend), die Demokratische Juristinnen und Juristen (je weniger Verdacht, umso mehr Überwachung) oder die schweizerischen Datenschutzbeauftragten (Garantien für die Grundrechte ungenügend). Zustimmung signalisierten Polizeiorganisationen wie die Konferenz der kantonalen Polizeikommandanten der Schweiz, der Verband Schweizerischer Polizeibeamter oder die Konferenz der städtischen Polizeidirektorinnen und Polizeidirektoren. Die Strafverfolgungsorgane sehen einerseits in den bestehenden Strukturen noch Steigerungspotenzial, anerkennen anderseits aber die Notwendigkeit angepasster Aufklärungsmethoden und weisen auf die grundlegende Bedeutung des Rechtsschutzes hin.

Im Zentrum der Kritik steht die Notwendigkeit der Vorlage als solches. Weitere Grundsatzkritik betreffen fehlende gesetzliche Definitionen von Terrorismus und gewalttätigem Extremismus, das Anordnungs- und Genehmigungsverfahren für die besondere Informationsbeschaffung (z.B. seien Verfahren bzw. Begriff der Stellungnahme des Bundesverwaltungsgerichts und seine Bindungswirkung unklar) und den Rechtsschutz (z.B. fehlende Kognition des Bundesverwaltungsgerichts verhindere wirksame Beschwerdeführung).

Anlass zu (eher punktueller) Kritik geben sodann die elektronische Lagedarstellung (z.B. es handle sich um eine Datensammlung gemäss Datenschutzgesetz), die bundesrechtliche Regelung der Einsicht kantonaler Kontrollbehörden in Daten des Bundes (z.B. mit Organisationsautonomie der Kantone/Städte/Gemeinden nicht vereinbar), die Auskunftspflichten von Behörden und gewerblichen Transporteuren (z.B. Notwendigkeit für eine zeitlich unbefristete Regelung unklar), die Regelungen

über Informantinnen und Informanten (z.B. kein Anreizsystem für Privatpersonen) sowie der Tarnidentitäten (z.B. Tarnidentitäten nur bei Strafverfahren), der absolute Quellenschutz (z.B. kein Schutz für straffällige oder bösgläubige Informantinnen und Informanten), die besonderen Mittel der Informationsbeschaffung (z.B. Ausdehnung des Geltungsbereichs auf gewalttätigen Extremismus/organisierte Kriminalität prüfen), die nachträgliche Mitteilungspflicht (z.B. Verhältnis zwischen nachträglicher Informationspflicht und indirektem Auskunftsrecht klärungsbedürftig), das Dringlichkeitsverfahren (z.B. Sicherstellung der Vernichtung von bereits ins Ausland übermittelten Daten im Falle der späteren Nichtgenehmigung einer Massnahme), das Tätigkeitsverbot (z.B. kein Verbot von Tätigkeiten ohne strafrechtlich relevantes Handeln).

1.4.2 Überarbeitung des Vorentwurfes

Der Bundesrat nahm am 4. April 2007 vom Ergebnis des Vernehmlassungsverfahrens Kenntnis und beauftragte das EJPD mit der Ausarbeitung einer Botschaft; gleichzeitig legte er Grundsätze für die weitere Ausgestaltung der Vorlage fest.

Für die Ausarbeitung der Botschaft diente der Vernehmlassungsentwurf als Grundlage, wobei die wesentlichen Einwände, Bemerkungen und Vorschläge der Vernehmlassung umfangreich eingearbeitet wurden.

Die wichtigsten Änderungen gegenüber dem Vernehmlassungsentwurf sind:

- die Überarbeitung und Vertiefung der auf die Notwendigkeit der Vorlage zielenden Argumentation und der als unklar gerügten Begriffe und Verfahrensabläufe, insbesondere des Verfahrens vor Bundesverwaltungsgericht und die Entscheidfindung der Exekutive;
- die wirksame Stärkung des Rechtsschutzes durch erweiterte Kognition des Bundesverwaltungsgerichts;
- der Verzicht auf eine bundesrechtliche Regelung für die Einsicht kantonaler Kontrollbehörden in Daten des Bundes;
- der Verzicht auf einen umfassenden Quellenschutz;
- die Ausgestaltung der elektronischen Lagedarstellung als Datensammlung gemäss Datenschutzgesetz;
- die Festlegung der Schriftform für die Zusicherung des ersuchenden Staates beim sog. Clearing.

Auf eine Harmonisierung des Quellenschutzes zwischen DAP und SND wurde zur Zeit noch verzichtet. Einerseits wurde in der Vernehmlassung die Angst geäussert, im Falle eines Wechsels vom relativen zum absoluten Quellenschutz könnten bösgläubige Denunziantinnen und Denunzianten durch wahrheitswidrige Äusserungen unbescholtene Bürger zu Unrecht in Verruf bringen. In diese Richtung zielten andererseits auch die Überlegungen des seinerzeitigen Gesetzgebers, der u.a. mit Blick auf Gewährspersonen, die sich selber strafbar gemacht haben könnten, von einer solchen Bestimmung absah. Vor allem jedoch erlaubt die für den DAP geltende Regelung bereits heute weitgehend, den Quellenschutz den jeweiligen Bedürfnissen anzupassen, und vermeidet Ungereimtheiten im Bereich der Aufsicht.

Intensiv geprüft und verworfen wurde weiter die von verschiedenen Vernehmlassungsteilnehmerinnen und -teilnehmern geforderte gesetzliche Definition der Begriffe «Terrorismus» und «gewalttätiger Extremismus». Die Ablehnung gründet vor allem auf zwei Überlegungen: Zum einen ist in der Vollzugsverordnung (VWIS) umschrieben, was unter «terroristische Aktivitäten» bzw. «gewalttätigem Extremismus» zu verstehen ist («Bestrebungen zur Beeinflussung oder Veränderung von Staat und Gesellschaft, die durch die Begehung oder Androhung von schweren Straftaten sowie mit der Verbreitung von Furcht und Schrecken verwirklicht oder begünstigt werden sollen» bzw. «Bestrebungen von Organisationen, deren Vertreter die Demokratie, die Menschenrechte oder den Rechtsstaat ablehnen und zum Erreichen ihrer Ziele Gewalttaten verüben, befürworten oder fördern»). Es bestehen mit anderen Worten bereits präzise Umschreibungen der einschlägigen Aktivitäten; von einem konturlosen unbestimmten Rechtsbegriff kann nicht die Rede sein. Zum anderen gibt es bis heute keine umfassende international anerkannte Definition des Begriffs Terrorismus. Mit der Schaffung einer entsprechenden Definition würde der Entwicklung des internationalen Rechts vorgegriffen, wodurch die Flexibilität der nationalen Gesetzgebung im Verhältnis zum internationalen Recht verloren ginge. Auch kann mit der Regelung auf Verordnungsstufe schneller und einfacher der Weiterentwicklung des internationalen Rechts Rechnung getragen werden. Hinzu kommt, dass die Abgrenzung zu Freiheitskämpfern oder Staatsterrorismus noch nicht abschliessend geklärt ist. Der von der Europäischen Union angenommene Rahmenbeschluss (Rahmenbeschluss 2002/475/JI) bestimmt die terroristischen Straftaten und die Sanktionen, die Mitgliedstaaten in ihren nationalen Rechtsvorschriften vorsehen müssen. Das Ziel ist somit eine Angleichung der tatbestandsmässigen Umschreibung der terroristischen Straftaten. Dies wirkt sich jedoch nicht im nachrichtendienstlichen Bereich (Prävention), sondern einzig bei der Strafverfolgung (Repression) aus.

Ferner wurde der Gesetzestext unter Berücksichtigung der inzwischen in Kraft getretenen BWIS-Revision betreffend Gewalt an Sportveranstaltungen und Gewaltpropaganda strukturell bereinigt.

1.5 Abstimmung von Aufgaben und Finanzen

Sicherheit ist nicht kostenlos (Bericht USIS II, Strategische These 10). Die Kosten erfolgreicher Präventionsarbeit sind jedoch immer sehr viel tiefer als der für die Verwirklichung eines Risikos (z.B. eines Terroranschlages) zu zahlende Preis (Tote, Verletzte, materielle Schäden, Verunsicherung der Bevölkerung, Auswirkungen auf die Wirtschaft usw.). Selbst nach einer Aufstockung um 40 Stellen (der DAP zählt heute rund 140 Stellen, wovon rund 90 im Kernbereich des präventiven Staatsschutzes nach BWIS) bleibt der präventive Staatsschutz im europäischen Vergleich sowohl in absoluten (Anzahl Stellen total) als auch in prozentualen Zahlen (Anzahl pro Einwohnerinnen und Einwohner) weit unter der Grösse der Dienste vergleichbarer Länder (z.B. Österreich, Belgien, Holland, Dänemark). Er profitiert durch seine polizeiliche Verankerung weiterhin von umfangreichen Synergien mit dem föderalistischen Polizeisystem der Schweiz.

Alles in allem rechtfertigen die auf dem Spiele stehenden Interessen und Werte die mit der Umsetzung der Gesetzesrevision verbundenen Kosten.

1.6 Rechtsvergleich und Verhältnis zum europäischen Recht

1.6.1 Allgemeines

Die bestehenden und im Nachgang zu den Terroranschlägen vom 11. September 2001 erlassenen bzw. oft verschärften ausländischen Gesetzgebungen können angesichts der unterschiedlichen Gefährdungslagen, politischen Systemen und der landesspezifischen Erfahrung mit dem Terrorismus in den jeweiligen Staaten (z.B. Spanien/ETA) nicht unbesehen auf die Schweiz übertragen werden.

Die Zunahme der terroristischen Bedrohung hat generell zu einer verstärkten Zusammenarbeit der für die innere Sicherheit zuständigen Dienste der internationalen Gemeinschaft geführt. Diese hat die Notwendigkeit erkannt, im Kampf gegen den Terrorismus gemeinsam zu handeln und die internationale Zusammenarbeit in diesem Bereich zu institutionalisieren. So dient beispielsweise die vom «Club de Berne» geschaffene «Counter Terrorist Group/CTG» als Schnittstelle zwischen der EU und den Leitern der Sicherheits- und Nachrichtendienste der Mitgliedsstaaten.

Das Schweizerische Institut für Rechtsvergleichung (SIR) verglich Anfang 2003 und Mitte 2005 die rechtlichen Grundlagen der inneren Sicherheit in den wichtigsten europäischen Ländern.

Die Gesetzgebung in allen nachfolgend erwähnten Ländern ist geprägt durch die Ereignisse des 11. Septembers 2001 in den USA.

Die organisatorischen Strukturen und die politischen und rechtlichen Handlungsmöglichkeiten unterscheiden sich von Staat zu Staat. Es ist deshalb nicht einfach, klare Vergleiche und Schlussfolgerungen für die Schweiz zu ziehen. Im Folgenden werden die gesetzlich geregelten Massnahmen und Kompetenzen in ausgewählten Ländern sowie der jeweils vorhandene Rechtsschutz bzw. das Kontrollsystem vereinfacht in zwei Tabellen dargestellt. Ausführlichere Erklärungen dazu befinden sich im Anhang 1. Das Fehlen einer ausdrücklichen gesetzlichen Regelung bedeutet dabei nicht, dass die erwähnte Massnahme im betreffenden Land nicht zur Anwendung kommt. Sie wird möglicherweise als nicht regelungsbedürftig betrachtet oder ist in anderen Regelungen miterfasst.

1.6.2 Rechtsvergleich mit dem Ausland

Massnahme	Repression/Strafverfolgung	Prävention
Funkaufklärung Art. 14*a* Entwurf		Deutschland, Frankreich, Italien, Niederlande
Entschädigung von Informanten Art. 14*b* Entwurf	Frankreich, Italien	Italien, Frankreich
Schutz von Informanten Art. 14*c* Entwurf	Österreich, Deutschland, Frankreich, Italien	Österreich, Deutschland, Frankreich, Niederlande
Tarnidentität Art. 14*d* Entwurf	Österreich, Deutschland, Frankreich, Italien, Niederlande	Österreich, Deutschland, Frankreich, Niederlande
Überwachung des Brief-,Post- und Fernmeldeverkehrs Art. 18*k* Entwurf	Österreich, Deutschland, Frankreich, Italien, Luxemburg, Niederlande	Deutschland, Frankreich (nicht Postüberwachung), Italien, Luxemburg, Niederlande
Observierung von privaten Räumen Art. 18*l* Entwurf	Österreich, Deutschland, Frankreich, Italien, Luxemburg, Niederlande	Österreich, Deutschland, Frankreich, Italien, Niederlande
Eindringen in elektronische Systeme Art. 18*m* Entwurf	Deutschland, Frankreich, Luxemburg, Niederlande	Frankreich, Niederlande
Verbot bestimmter Tätigkeiten gegen Einzelpersonen oder Gruppen Art. 18*n* Entwurf	Österreich, Deutschland, Italien, Luxemburg, Niederlande	Frankreich, Deutschland, Österreich

1.6.3 Rechtsschutz und institutionelle Kontrollen im Ausland

Länder	Ordentliche Kontrolle	Besondere Kontrolle
Deutschland	*Allgemein:* Oberaufsicht des Datenschutzbeauftragten, parlamentarische Kontrolle; Verpflichtungsklage beim Verwaltungsgericht.	*Überwachung des Brief-, Post- und Fernmeldeverkehrs:* Antrag durch Präsident des BfV oder Vertreter, Anordnung Bundesministerium; Überprüfungsinstanz: G 10-Kommission. Ausnahme: Gefahr in Verzuge, dann sofortiger Vollzug, nachträgliche Information der Kommission. *Tarnidentität:* Zustimmung des Bundesministers des Innern.
Österreich	Möglichkeit der Beschwerde bei Datenschutzkommission, beim Verwaltungsgerichts- oder Verfassungsgerichtshof.	*Allgemein:* Kontrolle des Rechtschutzbeauftragten; parlamentarische Kontrolle, Sicherheitsbehörden informieren Bundesminister für Inneres unverzüglich. *Verdeckte Ermittlung und verdeckter Einsatz von Bild- und Tonaufzeichnungsgeräten:* Begleitete Kontrolle durch Rechtschutzbeauftragten.

Länder	Ordentliche Kontrolle	Besondere Kontrolle
Frankreich	Einsichtsgesuche an «Commission nationale de l'information et des libertés» (CNIL).	*Überwachung des Brief und Fernmeldeverkehrs:* Antrag des Verteidigungsministers, des Innenministers und des Ministers für Zollwesen oder ihrer Stellvertreter; Anordnung durch Premierminister oder zweier durch ihn ernannter Personen. *Überprüfungsinstanz:* Verwaltungsunabhängige «Commission nationale de contrôle des interceptions de sécurité».
Italien	Regierung liefert dem Parlament pro Semester ein Rechenschaftsbericht über die Aktivitäten der Dienste. Datenschützer (Garante per la protezione dei dati personali) übt Kontrolle der gesammelten Daten aus.	*Überwachung des Brief-, Post- und Fernmeldeverkehrs:* Antrag durch den Ministerpräsidenten, Einwilligung des Richters. Ministerpräsident kann seine Befugnisse an die Dienste delegieren; Anordnung durch Staatsanwaltschaft. Bei Gefahr in Verzug sofortige Anordnung. Spätestens nach 24 Stunden muss dem Richter auf dem ordentlichen Weg die Bewilligung eingeholt werden. Richter muss innerhalb von 48 Stunden über den Antrag entscheiden.
Luxemburg	Parlamentarischen Kontrollkommission; Aufsichtskontrolle der Daten durch den Generalstaatsanwalt oder einer seiner Delegierten und zwei vom Minister gewählten Vertreter einer Spezialkommission; Oberste Datenschutzstelle (ANS) wacht über Sicherheit der klassifizierten Daten.	*Überwachung des Brief-, Post- und Fernmeldeverkehrs:* Antrag durch SRDE im Einverständnis einer Spezialkommission; Anordnung durch Direktor der Telekommunikationsdienste, welcher die Abhörungen durch eine dafür geschaffene Stelle vollziehen und kontrollieren lässt. Die parlamentarische Kontrollkommission wird alle sechs Monate über die durchgeführten Massnahmen betreffend die Telefonüberwachung informiert.
Niederlande	Aufsichtskommission; unabhängiger Ombudsmann. Parlamentarischen Aufsichtskommission *Tarnidentität:* Briefe Dritter öffnen erlaubt, sofern das Bezirksgericht Den Haag einem Antrag des Chefs der Dienste entspricht.	*Überwachung des Brief-, Post- und Fernmeldeverkehrs:* Antrag durch Chef AIVD und MIVD, Anordnung durch Innenminister. Bei Gefahr in Verzug, ist eine nachträgliche Genehmigung erlaubt, wenn diese so schnell wie möglich eingeholt wird. *Observierung:* Allgemein bei schriftlicher Einwilligung des zuständigen Ministers. Observation privater Räume. in Absprache mit dem Innenminister oder dem Chef der Dienste erlaubt.

1.6.4 Vergleich mit der Schweiz

Die Sicherheitsstrukturen und die rechtlichen Handlungsmöglichkeiten der Sicherheitsbehörden unterscheiden sich zwar von Staat zu Staat. Dennoch ergibt sich aus dem Rechtsvergleich, dass die heutigen schweizerischen Präventionsmassnahmen und die verfügbaren Ressourcen deutlich unter den Möglichkeiten liegen, die in zahlreichen westeuropäischen Ländern zulässig sind.

Damit entstehen gefährliche und international spürbare Lücken. Dies kann eine illegale Nachrichtenbeschaffung ausländischer Behörden auf Schweizergebiet zur Folge haben. In mehreren Fällen ist dies bereits geschehen.

Eine ungenügende Fähigkeit zur Früherkennung im eigenen Land und zur internationalen Zusammenarbeit kann zudem dazu führen, dass sich die Schweiz selber schadet, weil ihr wichtige Informationen nicht mehr bereitwillig weitergegeben werden. Das könnte zu einer zusätzlichen Schwächung der schweizerischen Terrorabwehr führen.

Die Erfahrung der letzten Anschläge zeigt, dass die Netzwerke des Terrorismus bei Brüchen in der Zusammenarbeit viel zu spät erkannt werden. In Fällen verhinderter Terroranschläge kamen häufig Informationsbeschaffungsmittel zum Einsatz, die in der Schweiz heute präventiv nicht zur Verfügung stehen. So beispielsweise beim geplanten Attentat auf den Weihnachtsmarkt von Strassburg im Jahre 2000, bei der Entdeckung des Rizin-Pflanzengift-Labors in London (2003), bei der Aufdeckung des islamistischen Hofstad-Netzwerkes in Holland (2003) oder beim verhinderten Anschlag auf die Einweihung des jüdischen Kulturzentrums durch die Neonazigruppe «Kameradschaft Süd» in Deutschland (2003).

Die Schweiz muss in der Lage sein, auf einem minimalen de-facto-Standard der europäischen Staaten zu arbeiten. Auf weitergehende Massnahmen wird vorläufig verzichtet.

1.7 Umsetzung

Für die Umsetzung der Massnahmen kann beinahe vollumfänglich auf die bestehenden eidgenössischen (Bundesverwaltungsgericht, DAP, Dienst für besondere Aufgaben UVEK) und kantonalen Strukturen (kantonale Polizei- und Sicherheitsbehörden) aufgebaut werden.

1.8 Erledigung parlamentarischer Vorstösse

Die Motion Burkhalter[33] verlangt, dem Parlament seien die für eine bessere präventive Terrorismusbekämpfung notwendigen Gesetzesänderungen zu unterbreiten. Wiewohl diesem Anliegen mit der vorliegenden Botschaft entsprochen wird, kann keine Abschreibung erfolgen, da die Motion bekämpft wird und sie in den Räten bisher noch nicht behandelt wurde.

2 Erläuterungen zu den einzelnen Artikeln

Allgemeine Systematik

Die aktuelle Revision des BWIS erfordert eine Änderung der Gesetzessystematik. Die bisherigen (und weiter bestehenden) «einfachen» Informationsbeschaffungsmittel sollen sich klar von den «besonderen» Mitteln der Informationsbeschaffung und deren Anordnungsvoraussetzungen unterscheiden. Deshalb wird das Gesetz um das

33 04.3216 Motion Burkhalter. Terrorismusbekämpfung. Präventive Massnahmen.

Kapitel «Besondere Informationsbeschaffung» mit den zwei Abschnitten: «Allgemeine Bestimmungen» und «Besondere Mittel der Informationsbeschaffung» erweitert. Im ersten Abschnitt des neuen Kapitels finden sich die allgemeinen Anordnungsvoraussetzungen der besonderen Informationsbeschaffungsmittel; der zweite Abschnitt befasst sich mit den jeweiligen Mitteln im Einzelnen, d.h. der Überwachung des Post- und Fernmeldeverkehrs, dem Beobachten an nicht allgemein zugänglichen Orten (auch mittels technischem Überwachungsgerät) sowie dem geheimen Durchsuchen von Datenverarbeitungssystemen. Die Neugliederung bedingt auch die Verschiebung des durch Ziffer I des BG vom 24. März 2006 (in Kraft seit 1. Januar 2007) eingefügten Artikels 13*a* (vgl. nachfolgenden Kommentar zum Art. 18*o*).

Art. 2 Abs. 4 Bst. b^{bis} und b^{ter}

Das geltende Gesetz zählt die vorbeugenden Massnahmen in Artikel 2 Absatz 4 abschliessend auf. Diese Auflistung ist mit den neu eingeführten, in Kapitel 3*a* geregelten besonderen Mitteln der Informationsbeschaffung (Bst. b^{bis}) und dem Tätigkeitsverbot (Bst. b^{ter}) gemäss Kapitel 3*b* zu ergänzen.

Art. 7 Abs. 2, dritter Satz

Nach Artikel 7 Absatz 2 BWIS erfüllen die Kantone die Aufträge nach diesem Gesetz selbstständig. Müssen mehrere Kantone mitwirken oder ist Gefahr in Verzug, kann das Bundesamt für Polizei die Leitung übernehmen. Diese Kompetenz soll dahingehend ergänzt werden, dass das Bundesamt für Polizei den Austausch von Informationen koordinieren kann, wenn dadurch die Arbeit bei Bund und Kantonen massgeblich erleichtert wird. Das Bundesamt für Polizei stellt also einen koordinierten Informationsaustausch zwischen (kantonalen) Verwaltungseinheiten sicher, die originär zuständig sind und es auch bleiben. Der Begriff Koordination soll den kooperativen Charakter der Massnahme verdeutlichen. Das Kriterium der Massgeblichkeit besagt, dass beim gegenseitigen Informationsaustausch ein klares Plus resultieren muss. Demnach soll die durch das Bundesamt für Polizei sichergestellte Kooperation das Informationsaufkommen aller beteiligten Stellen erheblich verbessern. Im Übrigen handelt es sich um eine Kann-Bestimmung; eine Pflicht zur Übernahme der Koordination besteht für das Bundesamt für Polizei keine.

Öffentliches Interesse und Verhältnismässigkeit

Mit der zunehmenden Internationalisierung der terroristischen und gewaltextremistischen Ideologien und ihrer militanten Anhängerschaft wird die präventive Gefahrenabwehr immer schwieriger. Deshalb rechtfertigt es sich, die koordinierende Funktion des Bundesamts für Polizei bei der Wahrnehmung der ihm gesetzlich übertragenen Aufgaben anzupassen. Um eine entsprechende Gefährdung frühzeitig zu erkennen, sind umfassende Kenntnisse der komplexen, oft grenzüberschreitenden Vorgänge und personellen Verflechtungen unabdingbar. Als entscheidend erweist sich ein intensiver Informationsaustausch mit ausländischen Partnerbehörden. Die nun vorgeschlagene Koordination respektiert das verfassungsmässige Subsidiaritätsprinzip, das für die Aufgabenteilung zwischen Bund und den Kantonen mit massgebend ist (vgl. den neuen Art. 5*a* BV, welcher im November 2004 vom Volk und den Ständen angenommen wurde und voraussichtlich am 1. Januar 2008 in Kraft treten wird).

Kapitel 3: Allgemeine Informationsbeschaffung und -bearbeitung

Bedingt durch die neue Gesetzessystematik wird der bisherige 3. Abschnitt («Informationsbearbeitung») neu zum Kapitel 3: «Allgemeine Informationsbeschaffung und -bearbeitung».

Mit der angepassten Überschrift des neu eingefügten 3. Kapitels soll die Abgrenzung zur besonderen Informationsbeschaffung besser hervorgehoben werden. Dabei ist die «Allgemeine Informationsbeschaffung und -bearbeitung» identisch mit der heute zulässigen Informationsbeschaffung, die sich an der Amtshilfe unter Behörden orientiert, kaum in Grundrechte eingreift und dem präventivpolizeilichen Verständnis des Gesetzgebers von 1997 entspricht.

Am Kernstück des heutigen BWIS – der Regelung der Informationsbearbeitung – ändert die vorliegende Revision nichts. Die einschlägigen Regeln gelten weiterhin und auch für die mit den besonderen Mitteln der Informationsbeschaffung erhobenen Daten, soweit in Kapitel 3a nicht ausdrücklich Anderes vorgesehen wird.

Art. 10a Lagedarstellung

Die Bestimmung regelt eine Aufgabe, die bereits heute von den Sicherheitsorganen des Bundes wahrgenommen wird (vgl. die Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement[34] , insbesondere Art. 9 Abs. 2 Bst. a Ziff. 2, sowie Art. 15 Abs. 3 BWIS und Art. 4 Abs. 2 Bst. k der ISIS-Verordnung[35]).

Das Bundesamt für Polizei ist verantwortlich für die ständige Lagebearbeitung im Bereich der inneren Sicherheit. Dazu führt es das Bundeslagezentrum, das die relevante Lage aus den Teilbereichen der inneren Sicherheit (Kantone, andere Bundesstellen) zu einem Gesamtbild integriert. Das Bundeslagezentrum wirkt zudem bei besonderen Ereignissen (z.B. Grossanlässen) massgeblich an der Führung des nationalen Nachrichtenverbundes mit. Zur Aufgabenerfüllung betreibt es ein elektronisches Informationssystem. Technische Verbindung zwischen dem Staatsschutz-Informations-System (ISIS) und dem Lageinformationssystem besteht keine. Soweit dies zur Lagedarstellung erforderlich ist, kann das System auch besonders schützenswerte Personendaten (vgl. Art. 3 des Bundesgesetzes vom 19. Juni Bundesgesetzes vom 19. Juni 1992[36] über den Datenschutz [DSG]) enthalten.

Art. 13 Sachüberschrift, Abs. 3 und 4 Allgemeine Auskunftspflicht der Behörden

Die Einführung von Artikel 13*a* bedingt eine Anpassung von Artikel 13, damit der Unterschied zwischen den beiden Formen der Auskunftspflicht besser erkennbar wird.

Sachüberschrift

Mit der Änderung der Sachüberschrift von Artikel 13 – insbesondere dem Wort «Allgemeine» – wird zum Ausdruck gebracht, dass die Auskunftspflicht für den gesamten Aufgabenbereich des BWIS gilt.

34 SR **172.213.1**
35 SR **120.3**
36 SR **235.1**

Abs. 3

Da Erkenntnisse über eine Bedrohung durch Terrorismus, verbotenen politischen oder militärischen Nachrichtendienst, verbotenen Handel mit Waffen, radioaktiven Materialien oder durch verbotenen Technologietransfer dauerhaft mitzuteilen sind (vgl. Art. 13*a* nachfolgend), ist im Artikel 13 die Delegation an den Bundesrat auf die verbleibenden Bereiche zu beschränken. Es sind dies der gewalttätige Extremismus und der verbotene wirtschaftliche Nachrichtendienst.

Abs. 4

Die in diesem Absatz bisher enthaltene Regelung wird aufgehoben und neu als eigenständiger Artikel gegliedert (vgl. Art. 13*b* nachfolgend).

Art. 13a Besondere Auskunftspflicht der Behörden

Der geltende Artikel 13*a* BWIS (Sicherstellung, Beschlagnahme und Einziehung von Propagandamaterial) wird aufgrund der geänderten Gesetzessystematik neu zu Artikel 18*o*; mit der Verschiebung innerhalb des Gesetzes geht keine materielle Änderung einher (vgl. Erläuterung zu Art. 18*o*).

Bezogen auf Artikel 13 handelt es sich beim *neuen* Artikel 13*a* um eine Spezialnorm. Einerseits beschränkt sie sich auf einen Teilbereich des gesetzlichen Aufgabenbereichs. Anderseits geht sie weiter, indem sie für alle Behörden des Bundes, der Kantone und für Organisationen, die öffentliche Aufgaben wahrnehmen, Geltung beansprucht. Nicht darunter fallen aber beispielsweise Kantonalbanken, da diese nicht hoheitlich handeln.

Abs. 1

Dieser Absatz legt eine Auskunftspflicht für bestimmte Gefährdungen fest (vgl. Bst. a–c). Es geht dabei um Gefährdungen, die aufgrund ihres Potenzials die Grundwerte der Schweiz bedrohen können. Als solches richten sie sich gegen parlamentarische, richterliche oder Regierungsinstitutionen und stellen die Existenz oder das richtige Funktionieren der Schweiz in Frage. Werden Bürgerinnen und Bürger bei der Ausübung ihrer Volksrechte behindert oder eingeschüchtert, fördert dies ein Gefühl der Unsicherheit und der Staat läuft Gefahr, dass sein demokratisches System unterminiert wird. Bedrohungen der geschilderten Art kennzeichnen Terrorismus, verbotenen politischen und militärischen Nachrichtendienst und den verbotenen Handel mit Waffen oder radioaktiven Materialien sowie verbotenen Technologietransfer.

Die Bestimmung verpflichtet grundsätzlich alle Behörden und Verwaltungseinheiten des Bundes und der Kantone zur Auskunft. Dieser Adressatenkreis ergibt sich aus Artikel 13 Absatz 3 BWIS bzw. aus der Verordnung vom 7. November 2001[37] betreffend die Ausdehnung der Auskunftspflichten und des Melderechts von Behörden, Amtsstellen und Organisationen zur Gewährleistung der inneren und äusseren Sicherheit (sog. Auskunfts- und Meldeverordnung). Leitgedanke ist, dass wenn im eingeschränkten Anwendungsbereich dieser Bestimmung (Terrorismus, politischer und militärischer Nachrichtendienst, verbotener Handel mit Waffen oder radioaktiven Materialien und verbotener Technologietransfer) eine konkrete Gefahr für die Sicherheit der Schweiz vorliegt, sich das Gemeinwesen integral (Bund, Kantone,

37 SR **120.1**

Gemeinden) an der Gefahrenabwehr beteiligen soll. Zu den Verwaltungseinheiten des Bundes zählen zum Beispiel auch die Meldestelle für Geldwäscherei (MROS) oder die für Ausweise zuständigen Behörden. Zu den Verwaltungseinheiten der Kantone gehören diejenigen der Gemeinden; sie sind vom Begriff «Kanton» miterfasst. Organisationen, die öffentliche Aufgaben wahrnehmen, werden ebenfalls zur Auskunft verpflichtet. Gemäss Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[38] (RVOG) handelt es sich dabei um mit Verwaltungsaufgaben betraute Organisationen des öffentlichen oder privaten Rechts, die nicht der Bundesverwaltung angehören. Eine Auflistung der betroffenen Organisationen im Gesetz selber ist aus praktischen Gründen nicht möglich. Zudem wäre eine solche Auflistung in einem Gesetz zu einschränkend, weil gegebenenfalls den rasch ändernden Verhältnissen nicht rechtzeitig Rechnung getragen werden könnte. Deshalb soll von einer Auflistung im Gesetz abgesehen und stattdessen für die Bezeichnung der Organisationen, die der Auskunftspflicht unterstehen, eine Delegation an den Bundesrat vorgesehen werden (vgl. Abs. 3).

Mit der Formulierung «im Einzelfall» soll verdeutlicht werden, dass die zur Auskunft verpflichteten Behörden zwar dauerhaft, aber nur bezogen auf bestimmte, konkrete Einzelfälle und erst auf entsprechendes Auskunftsersuchen des Bundesamts für Polizei oder in seinem Auftrag handelnder kantonaler Sicherheitsorgane hin Auskunft zu erteilen haben. Weil die Auskunftspflicht nur einzelfallweise und einzig bezogen auf konkrete Gefahren gegeben ist, rechtfertigt sich auch der tendenziell breiter gefasste Adressatenkreis.

Die bei den Behörden und Organisationen eingeholten Auskünfte richten sich an das Bundesamt für Polizei; es ist der Empfänger. Die von den Kantonen mit Sicherheitsaufgaben betrauten Behörden können im Auftrag des Bundes tätig werden und unmittelbar bei den auskunftspflichtigen Behörden und Organisationen Auskünfte einholen, um sie dem Bundesamt für Polizei zur Verfügung zu stellen. Dieses Vorgehen ist mit dem im Gesetz vorgesehenen System kohärent (vgl. Art. 7 Abs. 1, 13 Abs. 1 und 14 Abs. 1 BWIS). Kommt es hinsichtlich der Auskunftspflicht zu einer Meinungsverschiedenheit, besteht diese zwischen der auskunftsverweigernden Behörde oder Organisation und dem Bundesamt für Polizei, nicht aber mit der kantonalen Behörde, die im Auftrag des Bundesamts für Polizei die umstrittene Auskunft einholen wollte.

Der Sicherheit von Experten des schweizerischen Expertenpools für zivile Friedensförderung und von Mitarbeiterinnen und Mitarbeitern, die humanitären oder im Menschenrechtsbereich tätigen Organisationen zur Verfügung gestellt wurden, ist während im Ausland laufender Missionen besondere Achtung zu schenken. Insbesondere gilt es allfälligen Vertraulichkeitsklauseln, speziellen Verhaltenscodices oder Standing operating Procedures (SOP) in geeigneter Form Rechnung zu tragen. Massgebend sind die jeweiligen Umstände des Einzelfalles.

Abs. 2

Artikel 13*a* regelt die Aufhebung des Amtsgeheimnisses. In diesem Zusammenhang machten die Sozialversicherungs- und Steuerbehörden geltend, in ihrem Bereich gehe es nicht bloss um die Aufhebung eines Amtsgeheimnisses, sondern um die Aufhebung eines qualifizierten Amtsgeheimnisses. Dies bedürfe einer speziellen Regelung.

38 SR **172.010**

Im Sozialversicherungsbereich ist die Datenweitergabe in den jeweiligen Spezialgesetzen detailliert geregelt und bildet eine in sich geschlossene, umfassende und abschliessende Ordnung. Entsprechend wird das Amtsgeheimnis gegenüber den Sicherheitsorganen von Bund und Kantonen in den jeweiligen Spezialerlassen aufgehoben, wenn und soweit die Bedingungen von Artikel 13*a* erfüllt sind. Analoge Regelungen in den jeweiligen Spezialgesetzen finden sich für Sozialhilfebehörden, Zivilgerichte, Strafgerichte, Strafuntersuchungsbehörden, Betreibungsämter und Steuerbehörden.

Weniger einheitlich präsentiert sich die Situation im Steuerbereich. Zwar finden sich in einigen Bestimmungen Vorschriften über die Geheimhaltungspflicht oder die Schweigepflicht, doch besteht für die Datenweitergabe kein mit dem Sozialversicherungsbereich vergleichbares System. Auch ist der Begriff des Steuergeheimnisses nirgends explizit definiert (Umschreibungen finden sich jedoch in der Literatur, so beispielsweise: «Steuergeheimnis ist jede einer mit steuerlichen Aufgaben betrauten Person in Ausübung ihrer hoheitlichen Tätigkeit anvertraute oder ihr sonst wie zur Kenntnis gelangte persönliche Tatsache eines Steuerpflichtigen, die Steuerakten sowie die Verhandlungen innerhalb der Steuerbehörden[39]»). Hingegen schützt das Steuergeheimnis über das allgemeine Amtsgeheimnis hinaus auch private Interessen (Persönlichkeitsschutz). Alles in allem rechtfertigt es sich deshalb, dem Steuergeheimnis mit einer Spezialregelung Rechnung zu tragen. Verankert wird vorab der Grundsatz, dass auch die Steuerbehörden auskunftspflichtig sind. Ansprechpartner für die Auskunftserteilung ist die für die jeweilige Steuer zuständige eidgenössische oder kantonale Behörde. Besteht zwischen dem Bundesamt und der zuständigen Behörde Einigkeit über die Auskunftspflicht, kann die Auskunft ohne weitere Formalitäten erteilt werden. Bei Dissens gelangt das Verfahren nach Artikel 13*b* (Streitigkeiten über die Auskunftspflicht) zur Anwendung, d.h. der abschliessende Entscheid über die Auskunftspflicht obliegt bei eidgenössischen Steuern dem Bundesrat und bei kantonalen oder kommunalen Steuern dem Bundesverwaltungsgericht. Mit diesem Vorgehen kann auch eine gleichmässige Anwendung des Melderechts nach Artikel 13*a* Absatz 4 des Gesetzesentwurfs gefördert werden.

Abs. 3

Die Sicherheitsorgane entscheiden nicht alleine über die Auskunftspflicht einer Organisation. Deshalb soll der Bundesrat die verpflichteten Organisationen auf dem Verordnungsweg abschliessend bezeichnen.

Abs. 4

Die in Absatz 1 genannten Stellen, welche die in Absatz 3 erwähnten Stellen mitumfassen, sind auch ermächtigt, den mit Aufgaben nach dem BWIS befassten Behörden von Bund und Kantonen von sich aus Sachverhalte zu melden, von denen sie annehmen, dass eine Verbindung zu Terrorismus, verbotenem politischen oder militärischen Nachrichtendienst oder verbotenem Handel mit Waffen oder radioaktiven Materialien oder verbotenem Technologietransfer bestehen könnte. Die in Absatz 1 und 3 genannten Stellen sollen somit vor dem Vorwurf bewahrt werden, eine Amtsgeheimnisverletzung zu begehen. Es besteht indessen keine Pflicht für ein systematisches Meldewesen.

39 Weber, M.: Berufsgeheimnis im Steuerrecht und Steuergeheimnis, Zürich 1982, S. 139

Öffentliches Interesse und Verhältnismässigkeit

Mit dem neuen Artikel 13*a* soll die Bestimmung des heutigen Artikels 13 Absatz 3 BWIS auf Gesetzesstufe nachvollzogen werden. Es betrifft dies die Möglichkeit des Bundesrates, für begrenzte Zeit andere als die in Artikel 13 Absatz 1 BWIS aufgeführten Behörden der Auskunftspflicht zu unterstellen. Der Bundesrat machte davon Gebrauch, indem er die sog. Auskunfts- und Meldeverordnung erliess. Nach zweimaliger Verlängerung gilt diese Verordnung nun noch bis zum 31. Dezember 2008 (vgl. AS *2005* 5423).

Artikel 13 Absatz 3 BWIS, auf den sich die sog. Auskunfts- und Meldeverordnung stützt, verlangt eine zeitliche Befristung der entsprechenden Erlasse des Bundesrates. Die sich auf diese Bestimmungen abstützende Verordnung kann damit nicht beliebig verlängert werden. Sinn der vom Gesetzgeber vorgeschriebenen Befristung ist es, dass die Normen ins ordentliche Recht überführt werden, wenn deren Bestimmungen über einen längeren Zeitraum in Kraft bleiben sollen. Die nötige Gesetzgebung ist einzuleiten, sobald sich abzeichnet, dass die darin enthaltenen Regeln dauerhaft notwendig sind. Dieses Kriterium ist vorliegend erfüllt:

Nach den Anschlägen in Madrid 2004 erlangte die Bedrohung Europas durch den islamistischen Terrorismus im Juli 2005 eine neue Dimension.[40] Nach heutiger Beurteilung ist die Schweiz zwar nicht ein direktes und primäres Ziel des Terrorismus. Die allgemeine Gefahr für terroristische Aktionen hingegen bleibt weltweit gross, wovon auch die Schweiz – wie andere Länder – betroffen ist. Der Mittelmeerraum und Kontinentaleuropa sind nicht länger nur Ruhe- oder Vorbereitungsraum. Vielmehr ist davon auszugehen, dass Terrororganisationen bereit sind, bei sich bietender Gelegenheit mit terroristischen Anschlägen gegen westliche Interessen vorzugehen. Es ist mit einer langdauernden Auseinandersetzung zu rechnen; ein Ende der Bedrohung ist zum heutigen Zeitpunkt nicht absehbar.

Der Bundesrat beauftragte das EJPD im Dezember 2002, die Auskunfts- und Meldeverordnung auf ihre Wirksamkeit zu überprüfen und ihm Bericht zu erstatten. In der Folge wurde bei den Polizeikorps der Kantone und bei denjenigen der Städte Zürich und Bern eine Umfrage durchgeführt. Dabei wurde das Schwergewicht nicht auf das Meldeaufkommen als solches (Quantität), sondern auf den inhaltlichen Wert (Qualität) der Meldungen gelegt .

Zur Evaluation wurde ursprünglich beabsichtigt, die in einem Zusammenhang mit den erweiterten Befugnissen stehenden Meldungen im Staatsschutz-Informationssystem ISIS speziell zu kennzeichnen. Dieses Unterfangen stellte sich jedoch als viel zu aufwendig heraus, so dass darauf verzichtet werden musste. Zum anderen erwies es sich, dass mit der blossen Markierung von Meldungen die Auswirkungen der Auskunfts- und Meldeverordnung auf kantonaler Ebene gar nicht oder bloss unzureichend erfasst wurden. Dies namentlich in denjenigen Fällen, in denen auf kantonaler Ebene Meldungen dank der erweiterten Kompetenzen mit entsprechend kleinerem Aufwand abgeklärt werden konnten, ohne dass eine spezielle Meldung an den DAP erfolgte.

Weiter wurde festgestellt, dass die Auskunfts- und Meldeverordnung zwar auf polizeilicher Seite, nicht jedoch auf Seiten der zur Auskunft berechtigten oder verpflichteten Personen ausreichend bekannt war. Diesem Umstand wurde anlässlich

40 Bericht innere Sicherheit 2005 S. 27

der letzten Verlängerung mit einem entsprechend breit gestreuten Kreisschreiben Rechnung getragen.

Insgesamt ergab sich eine zahlenmässig eher geringe, inhaltlich jedoch deutliche Verbesserung des Meldeaufkommens.

Zusammenfassend erwies sich die Verordnung sowohl innen- wie auch aussenpolitisch von nicht zu unterschätzender Bedeutung (innenpolitisch: Gradmesser für den Willen des Bundesrates zum Kampf gegen den Terrorismus; aussenpolitisch: Signal für die Bereitschaft der Schweiz, ihre Rolle im internationalen Staatenverbund zur Bekämpfung des Terrorismus wahrzunehmen). Mit anderen Worten besteht an ihrer Weiterführung bzw. Überführung in das «ordentliche» Recht ein gewichtiges öffentliches Interesse.

Das zahlenmässig geringe, qualitativ aber hoch stehende Meldeaufkommen belegt die Verhältnismässigkeit der Massnahme.

Art. 13b Streitigkeiten über die Auskunftspflicht

Der Anwendungsbereich von Artikel 13*b* ist gegeben, wenn das Bundesamt für Polizei oder ein in seinem Auftrag tätiges kantonales Sicherheitsorgan gestützt auf Artikel 13 oder 13*a* eine Auskunft verlangt, die angefragte Stelle indessen nicht bereit ist, diese zu erteilen.

Abs. 1

Sind lediglich Verwaltungseinheiten der zentralen Bundesverwaltung (vgl. Art. 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[41] [RVOV]) hinsichtlich der Auskunftspflicht geteilter Meinung, entscheidet die gemeinsame Aufsichtsbehörde, das heisst der Vorsteher oder die Vorsteherin des antragstellenden Departements oder der Bundesrat (vgl. Art. 9 Abs. 3 des Bundesgesetzes über das Verwaltungsverfahren vom 20 Dezember 1968[42] [VWVG]). Käme es beispielsweise hinsichtlich einer Auskunft, die das Bundesamt für Polizei vom Bundesamt für Migration verlangt, zu Meinungsverschiedenheiten, so würde der Vorsteher oder die Vorsteherin des EJPD entscheiden.

Abs. 2

In allen übrigen Fällen kann das Bundesamt für Polizei an das Bundesverwaltungsgericht gelangen und um einen abschliessenden Entscheid ersuchen (vgl. die beantragte Ergänzung betr. Art. 35 Bst. d des Bundesgesetzes vom 17. Juni 2005[43] über das Bundesverwaltungsgericht). Dieser Weg steht dem Bundesamt für Polizei auch offen, wenn ein kantonales Sicherheitsorgan um die verweigerte Auskunft ersucht hat. Weil das kantonale Sicherheitsorgan im Auftrag des Bundes handelt, ist es folgerichtig, dass nicht das kantonale Sicherheitsorgan, sondern einzig das Bundesamt für Polizei an das Bundesverwaltungsgericht gelangen kann.

Das Verfahren vor dem Bundesverwaltungsgericht löst das bisherige Verfahren vor dem Bundesstrafgericht nach dem heutigen Artikel 13 Absatz 4 ab; die Klärung anderer Streitigkeiten über den Anwendungsbereich des BWIS soll nach dem neuen Artikel 29*a* ebenfalls dem Bundesverwaltungsgericht obliegen.

41 SR **172.010.1**
42 SR **172.021**
43 SR **173.32**

Streitigkeiten über die Auskunftspflicht können sich mit eidgenössischen oder kantonalen Behörden sowie mit Organisationen, die öffentliche Aufgaben wahrnehmen oder mit Stellen der dezentralen Bundesverwaltung (vgl. Art. 8 RVOV, z.B. BA) ergeben.

Art. 13c Auskunftspflicht gewerblicher Transporteure

Diese neu eingeführte Auskunftspflicht gleicht derjenigen nach Artikel 13*a*. Sie richtet sich an gewerbliche Transporteure. Der Adressatenkreis wurde aus Verhältnismässigkeitsgründen auf gewerbliche Transporteure eingeschränkt. Die Bestimmung gilt beispielsweise für Taxiunternehmen, Flug- und Eisenbahngesellschaften, Autovermietungen, Strassentransporteure usw. Gleich wie die Auskunftspflicht nach Artikel 13*a* knüpft die Auskunftspflicht gewerblicher Transporteure an bestimmte Bedrohungsformen an: Terrorismus, verbotener politischer und militärischer Nachrichtendienst, verbotener Handel mit Waffen oder radioaktiven Materialien sowie verbotener Technologietransfer.

Aktionen von erkannten gefährlichen Personen (z.B. Spione, Terroristen, im Proliferationsbereich tätige Ingenieure usw.) lassen sich rückwirkend oft nur mit Auskünften über ihr Mobilitätsverhalten erkennen (z.B. Unterlagen über Automiete usw.). Analoges gilt für unmittelbar bevorstehende oder bereits erfolgte Transporte von vermuteten Proliferationsgütern oder entsprechenden Technologietransfer.

Die Transporteure sind gehalten, Auskunft über bereits vorhandene, von ihnen für ihre eigenen Zwecke erhobene Daten zu erteilen. Artikel 13c verpflichtet sie somit nicht zur Erhebung zusätzlicher Daten. Da die Auskunftserteilung über ohnehin bereits vorhandenes Datenmaterial für die Transporteure keinen nennenswerten Mehraufwand verursacht, ist keine spezielle Entschädigung durch die Sicherheitsorgane vorgesehen; die Auskunft erfolgt unentgeltlich.

Mit der Formulierung «im Einzelfall» wird verdeutlicht, dass nur dann eine Auskunftspflicht besteht, wenn das Bundesamt für Polizei oder ein in seinem Auftrag handelndes kantonales Sicherheitsorgan in einem konkreten Einzelfall mit einem Auskunftsbegehren an den Transporteur gelangt.

Öffentliches Interesse und Verhältnismässigkeit

Nach Artikel 14 Absatz 2 Buchstabe b BWIS dürfen die Sicherheitsorgane für die Erfüllung ihrer Aufgaben Auskünfte einholen. Gelangen sie dafür an private Personen (seien es natürliche oder juristische), so verweigern diese teilweise unter Hinweis auf die Datenschutzgesetzgebung die Auskunft. Um im Bereich des für die Sicherheitsorgane besonders wichtigen gewerblichen Transportgewerbes solches zu verhindern, soll eine Auskunftspflicht für gewerbliche Transporteure eingeführt werden. Mit der Auskunftspflicht wird einerseits in die Berufssphäre des Transporteurs und andererseits in die Privatsphäre der so beobachteten Person eingegriffen. Es gilt deshalb zu prüfen, ob der Eingriff in Bezug auf das zur Diskussion stehende öffentliche Interesse verhältnismässig ist. Zu betonen ist, dass Erkenntnisse von privaten Transporteuren bei der Beurteilung einer potenziellen Gefährdung von ausschlaggebender Bedeutung sein können. Bewegungen bestimmter Personen (z.B. Angehörige ausländischer Tarnunternehmen) oder Güter (z.B. Transport von vermuteten Proliferationsgütern) oder Erkenntnisse über die Häufigkeit solcher Bewegungen erlauben oftmals erst, bestimmte konkrete Hinweise auf ihre Richtigkeit zu überprüfen. Es dürfte unbestritten sein, dass der Zugang zu dieser Art von Informationen ein ebenso geeignetes wie auch

notwendiges Mittel ist, damit das Bundesamt für Polizei die ihm übertragene präventive Gefahrenabwehr erfolgreich wahrnehmen kann.

Die Verhältnismässigkeit der Massnahme hängt von den konkreten Umständen des Einzelfalles ab. Wie bereits erwähnt, ist Grundvoraussetzung für die Auskunftspflicht gewerblicher Transporteure, dass die Auskunft im Einzelfall notwendig ist für das Erkennen und Abwehren einer konkreten Gefahr für die innere oder äussere Sicherheit der Schweiz, die in einem der oben erwähnten, bereits beschränkten, Aufgabengebiete des BWIS vorhanden ist. In diesem eng begrenzten Rahmen gilt es zu beachten, dass der Transporteur einzig gehalten ist, Auskunft über ihm bereits bekannte Informationen zu erteilen. Zur aktiven Informationsbeschaffung ist er nicht verpflichtet. Der Eingriff in seine Berufssphäre ist deshalb nicht unverhältnismässig. Weiter betrifft die Auskunft keinen durch ein Berufsgeheimnis oder einem speziellen Vertrauensverhältnis geschützten Bereich. Vielmehr geht es im Regelfall um Auskünfte über Vorgänge an allgemein zugänglichen Orten wie Strassen, Eisenbahnen usw. Ein unverhältnismässiger Eingriff in die Privatsphäre liegt auch hier nicht vor. Nichtsdestotrotz wird in der Praxis – gleich wie bei jedem anderen Grundrechtseingriff auch – in jedem konkreten Einzelfall das zu schützende öffentliche Interesse gegen das ebenso zu schützende private Interesse, insbesondere den Schutz der Privatsphäre, sorgfältig und umfassend gegeneinander abzuwägen sein. Im Ergebnis sollen also gewerbliche Transporteure nur zum Erkennen und Abwehren von wichtigen Gefahren zur Auskunft verpflichtet sein.

Art. 13d Berufsgeheimnis

Bestimmte Berufe können «nur dann richtig und einwandfrei ausgeübt werden, … wenn das Publikum auf Grund einer unbedingten Garantie der Verschwiegenheit das unentbehrliche Vertrauen zum Inhaber des Berufes hat.» (BGE *84* IV 108). Diese Voraussetzung wird zum einen durch die Strafbarkeit von Verletzungen eines Berufsgeheimnisses (beispielsweise Art. 321 StGB[44]; Art. 35 DSG) und zum andern durch die Einräumung des Rechts, auch gegenüber Behörden dem Berufsgeheimnis unterliegende Auskünfte zu verweigern, sichergestellt. Dieses Recht dient somit dem Schutz eines besonderen Vertrauensverhältnisses, welches nicht nur in gerichtlichen Verfahren, sondern immer dann zu beachten ist, wenn Private gegenüber Behörden zur Auskunft verpflichtet werden.

Das Berufsgeheimnis wird von der vorliegenden Revision nicht berührt. Dies wird entsprechend seiner Bedeutung in Artikel 13*d* unmissverständlich festgehalten. Folglich ist z.B. ein Kantonsarzt im Rahmen seiner Amtstätigkeit nach Artikel 13*a* zwar zu allgemeinen Auskünften verpflichtet, nicht aber zu Auskünften über sein unter die ärztliche Schweigepflicht fallendes Wissen.

Art. 14 Abs. 3

Artikel 14 BWIS listet die heute zulässigen Informationsbeschaffungsmittel, die kaum in die Grundrechte eingreifen, abschliessend auf. Während diese Mittel für die Informationsbeschaffung auch weiterhin von grosser Bedeutung sind und von den Sicherheitsorganen hauptsächlich angewendet werden sollen, können die in Kapitel 3*a* genannten besonderen Mittel zur Informationsbeschaffung nur unter bestimmten Umständen und subsidiär eingesetzt werden.

44 SR **311.0**

Abs. 3

Im geltenden Gesetz ist diese Bestimmung bedeutsam. Sie untersagt den Sicherheitsorganen im präventiven Bereich generell, strafprozessuale Zwangsmassnahmen anzuwenden oder in privaten Räumen Vorgänge zu beobachten. Mit der Revision soll nun der präventive Einsatz solcher Massnahmen ermöglicht werden, d.h. es sollen ausnahmsweise und unter streng restriktiven Bedingungen die Informationsbeschaffung mit besonderen Mitteln ermöglicht werden. Galt bisher also ein generelles Verbot, führt die Revision neu ein System der Ausnahmeregelung mit Bewilligungspflicht ein. Wiewohl es sich bei den besonderen neuen Mitteln nicht um Zwangsmittel im strafprozessualen Sinn, sondern um nachrichtendienstliche Informationsbeschaffungsmittel handelt, wird die Bestimmung in Absatz 3 hinfällig und ist deshalb aufzuheben. Die neu vorgesehene besondere Informationsbeschaffung ist aber sehr restriktiv ausgestaltet und unterliegt strengen Kontrollen durch Judikative und Exekutive (vgl. die Erläuterungen zu Kap. 3*a*).

Art. 14a Funkaufklärung

Die Sicherheitsorgane des Bundes befassen sich seit Jahrzehnten mit der Aufklärung von Funkausstrahlungen ausländischer Nachrichtendienste, welche mit nachrichtendienstlichen Bestrebungen gegen die Schweiz zusammenhängen können. Diese Ausstrahlungen finden zu einem grossen Teil nach wie vor im Spektrum der Kurzwelle statt und sind nicht besonders gegen den Empfang durch Dritte geschützt (vgl. hierzu auch Staatsschutzbericht 2000, S. 147 f.). Zum Zeitpunkt des Erlasses des BWIS wurde diese Tätigkeit deshalb unter die Beschaffung im Rahmen der Beobachtung von Vorgängen an öffentlichen und allgemein zugänglichen Orten gezählt (Art. 14 Abs. 2 Bst. f BWIS).

Unter Funkaufklärung gegen Ziele im Ausland ist heute generell die Erfassung von elektromagnetischen Ausstrahlungen zu verstehen, die im Ausland oder von Satelliten erzeugt werden und in der Schweiz empfangen werden können. Aktuell können solche Ausstrahlungen mit dem System ONYX im Bereich der Satellitenabstrahlungen und mit Kurzwellenempfangsanlagen in deren Frequenzspektrum erfasst werden. Welche Mittel und Systeme in Zukunft für einen Funkaufklärungsauftrag eingesetzt werden müssen, wird eine Frage der technischen Entwicklung sein. Der Gesetzestext schafft mit der allgemeinen Formulierung «Funkaufklärung» den notwendigen Raum, um auch weiterhin mit neuen technischen Entwicklungen Schritt halten zu können.

In den letzten Jahren hat das VBS mit dem Projekt ONYX Kapazitäten zur Aufklärung von Fernmeldeverkehr aufgebaut, der international via Satelliten übertragen wird. Dabei werden Ausstrahlungen der Satelliten auf die Erde erfasst und ausgewertet, die auch von den Fernmeldedienstleistern im Rahmen ihrer kommerziellen Tätigkeit erfasst und weiterverarbeitet werden. Seit April 2001 nimmt der DAP im Rahmen eines Testbetriebes an der Nutzung des Systems ONYX teil. Eine Rechtsgrundlage wurde hierzu in Artikel 9*a* VWIS geschaffen. Die Überführung dieser Bestimmung in das Gesetz soll mit der vorliegenden Revision erfolgen. Damit wird auch eine Forderung der Geschäftsprüfungsdelegation erfüllt, welche eine ausdrückliche gesetzliche Grundlage für die Nutzung von ONYX verlangt. Für die Nutzung der Funkaufklärung durch die Nachrichtendienste im VBS erfolgt parallel eine Änderung des Militärgesetzes (vgl. Änderung bisherigen Rechts, Ziff. 3, Art. 99 Abs. 1 und 1^{bis} und Art. 99*a* MG). Damit verfügen beide Nachrichtendienste in ihren

gesetzlichen Zuständigkeitsbereichen über formellgesetzliche Grundlagen für die Nutzung der Funkaufklärung.

Der neue Artikel 14*a* BWIS entspricht weitgehend der heutigen Regelung der VWIS. Er wurde mit der Möglichkeit zur allfälligen Überwachung von Inlandszielen ergänzt, die unter den Bedingungen und dem Verfahren nach den neuen Artikeln 18*d* und 18*e* erlaubt ist.

Abs. 1

Dieser Absatz ist die Grundlage dafür, dass das fedpol mit dem Mittel der Funkaufklärung Ziele im Ausland erfassen und die Erkenntnisse auswerten kann, und er definiert den Begriff der Funkaufklärung. Die Definition umfasst alle elektromagnetischen Ausstrahlungen aus dem Ausland. Eine Beschränkung auf bestimmte technische Anwendungen wie Kurzwelle oder ONYX wäre angesichts der rasanten Entwicklung der Telekommunikationstechnik in diesen Bereichen weder sachlich noch rechtlich sinnvoll.

Damit beruht die Nutzung von ONYX auf einer formellgesetzlichen Grundlage. Die Daten werden vom DAP originär erhoben, d.h. im Rahmen des eigenen gesetzlichen Auftrags. Mit der Datenerhebung wird das VBS beauftragt (vgl. den Kommentar zu Abs. 3).

Abs. 3

Die heutige Praxis der technischen Kooperation der Bundesstellen ist in dieser Bestimmung verankert. Sie ermächtigt das Bundesamt für Polizei, zum Vollzug der Funkaufklärung mit anderen Stellen des Bundes und der Kantone zusammenzuarbeiten. Das Fedpol betreibt nur in geringem Umfang eigene Anlagen für die Erfassung von Kurzwellenfunk und ist im Wesentlichen selbstständiger Auftraggeber der Abteilung Elektronische Kriegführung im VBS. Ein Anschluss an ein ausländisches Funküberwachungssystem (beispielsweise ECHELON) ist weiterhin nicht zulässig.

Abs. 4

Absatz 4 stellt sicher, dass im Bereich der ständigen Funkaufklärung in jedem Fall die Kontrollinstrumente gemäss Artikel 99 ff. des Militärgesetzes zur Anwendung kommen (vgl. Änderung bisherigen Rechts, Ziffer 3, Militärgesetz, insbesondere Art. 99*a*). Damit keine Diskrepanz zur Funkaufklärung zugunsten der Nachrichtendienste des VBS entsteht, soll die Kontrolle über die Aufklärung von reinen Auslandszielen weiterhin bei derselben Kontrollinstanz (unabhängige Kontrollinstanz/UKI) erfolgen. Bei allfälligen Inlandszielen muss jedoch das Verfahren gemäss Artikel 18*d* und 18*e* (vgl. unten) durchgeführt werden, soweit die Massnahme oder die Funkaufklärung Fernmeldeverkehr betrifft, der unter das Fernmeldegeheimnis fällt.

Öffentliches Interesse und Verhältnismässigkeit

Die Funkaufklärung ist ein Mittel zur Informationsbeschaffung aus Quellen, die grundsätzlich öffentlich zugänglich sind. Jedermann kann mit entsprechender Ausrüstung die Informationen empfangen. Der Einsatz dieses Mittels stellt deshalb keinen erheblichen Eingriff in die Privatsphäre dar und insbesondere auch keine Verletzung des Fernmeldegeheimnisses. Bestimmte Arten des Funkverkehrs, die mithilfe der Funkaufklärung überwacht werden können, fallen aber unter das Fernmeldegeheimnis. Hier kann die Funkaufklärung erheblich in die Privatsphäre ein-

greifen. In solchen Fällen kommen die Bestimmungen über die besonderen Mittel der Informationsbeschaffung zur Anwendung, insbesondere jene des Artikels 18*k* hinsichtlich der Überwachung des Post- oder Fernmeldeverkehrs. Weitere diesbezügliche Erwägungen finden sich in den Erläuterungen zu diesem Artikel.

Art. 14b Informantinnen und Informanten

Die Sicherheitsorgane sind zur Wahrnehmung ihrer Aufgaben auf Mitteilungen und Auskünfte von Personen angewiesen, die Zugang zu relevanten Informationen haben. Während das heutige BWIS den Einsatz von Informantinnen oder Informanten impliziert (vgl. insbesondere Art. 14 Abs. 2 Bst. b und d BWIS zum Einholen von Auskünften und Entgegennehmen von Meldungen), finden sich keine spezifischen Bestimmungen über deren Einsatz, deren Rechte, Pflichten oder über Leistungen seitens des Staats. Diese rudimentäre Rechtslage soll präzisiert werden.

Abs. 1

Damit wird dem Bundesamt für Polizei ausdrücklich erlaubt, Informantinnen und Informanten einzusetzen. Dabei handelt es sich um Personen, die freiwillig mit Sicherheitsorganen zusammenzuarbeiten, ohne dass damit ein Arbeitsvertrag im Sinne von Artikel 319 des Obligationenrechts[45] (OR) oder des Bundespersonalrechts zu Stande kommt. Der Umstand, dass diesen Personen Auslagen erstattet oder Prämien entrichtet werden (vgl. Abs. 2), ist kein Grund dafür, dieses Verhältnis als Arbeitsvertrag zu qualifizieren. Für einen Arbeitsvertrag im Sinne von Artikel 319 OR bedürfte es weiterer konstituierender Elemente wie beispielsweise eines formalrechtlichen Unterordnungsverhältnisses, wodurch die Informantin oder der Informant personalrechtlich, organisatorisch und zeitlich vom Bundesamt für Polizei abhängig würde. Eine solche Eingliederung in eine fremde Arbeitsorganisation ist klar nicht der Fall.

Abs. 2

Damit Informantinnen oder Informanten, welche die Staatsschutzorgane mehr oder weniger regelmässig mit Informationen versorgen, durch ihre Tätigkeit keine finanziellen Einbussen erleiden, werden ihnen ihre Auslagen zurückerstattet. Es handelt sich bei diesen Entschädigungen nicht um steuerbares Einkommen oder Lohn im Sinne der AHV-Gesetzgebung. Unkosten sind Auslagen, die der Informantin und dem Informanten bei der Ausführung ihrer Tätigkeit entstehen, namentlich Kosten für Reisen oder Telekommunikation.

Zudem können Informantinnen und Informanten für besonders wichtige Informationen fallweise Prämien erhalten. Die Prämien bewegen sich in der schon heute geübten Praxis auf einem bescheidenen Niveau von höchstens wenigen Tausend Franken jährlich und erreichen die Höhe eines existenzerhaltenden Einkommens bei Weitem nicht. Damit kein falsch verstandener Erfolgsdruck entsteht, soll der finanzielle Anreiz für die Tätigkeit einer Informantin oder eines Informanten erklärtermassen nicht ausschlaggebend sein. Bescheidene Prämien werden entrichtet, wenn die Person Informationen geben kann, welche die weitere Informationsbeschaffung oder die Beurteilung der Gefährdungslage wesentlich erleichtern.

45 SR **220**

Abs. 3

Das Verhältnis der Sicherheitsorgane zu Informantinnen und Informanten beruht auf gegenseitigem Vertrauen und auf der Vertraulichkeit der Beziehung nach aussen. Würde ihre Tätigkeit zugunsten der Sicherheitsorgane der Zielperson bekannt, wären sie entsprechend den staatsschutzrelevanten Einsatzgebieten höchsten Risiken ausgesetzt. Sie können deshalb weder in Personalakten des Amtes figurieren, noch bei Sozialversicherungen gemeldet werden (und sei es auch nur zur Feststellung, dass sie von der Versicherungspflicht befreit sind). Hingegen wird ihr Einsatz schon heute vom EJPD und von der Geschäftsprüfungsdelegation als ordentliche Kontrollorgane des BWIS auf Rechtmässigkeit und Zweckmässigkeit hin kontrolliert. Mit Absatz 3 soll neu klargestellt werden, dass allfällige Entschädigungen keiner Abgabepflicht unterliegen, wenn und soweit es für den Quellenschutz oder die weitere Informationsbeschaffung notwendig ist. Weder die Betroffenen noch das Gemeinwesen erleiden dadurch einen spürbaren Schaden, da es sich im Einzelnen wie auch insgesamt um geringe Beträge handelt; der Verwaltungsaufwand für deren Erfassung und Erhebung würde die zu erwartenden Beiträge um ein Vielfaches übersteigen.

Art. 14c Schutz von Informantinnen und Informanten

Das Ziel dieser Massnahmen ist der Schutz von Personen, die für die Beschaffung von Informationen für die Zwecke des BWIS Risiken auf sich nehmen. Darunter fallen namentlich zwei Personengruppen: Einerseits geht es um den Schutz von Personen, die von sich aus mit den Sicherheitsorganen kooperieren und deswegen Repressalien befürchten müssen. Andererseits soll mit der Gewährung entsprechenden Schutzes aussagewilligen Personen die Kooperation ermöglicht bzw. erleichtert werden, um so notwendige Informationen zu beschaffen. Damit wird vermieden, dass (wie dies in der Vergangenheit in der Schweiz bereits mehrfach geschah) hochkarätige aussagewillige Informanten an ausländische Nachrichtendienste, die entsprechenden Schutz gewähren können, «abgegeben» werden müssen, weil die Schweiz über keine entsprechenden Schutzmöglichkeiten verfügt.

Personen, die von sich aus mit den Sicherheitsorganen kooperieren, gehen unter Umständen erhebliche Risiken ein und müssen Nachstellungen befürchten, sei es aus ihrem persönlichen Umfeld (zum Beispiel Informantinnen und Informanten aus dem hiesigen Umfeld gewalttätiger Gruppierungen), sei es durch fremde Staaten (beispielsweise menschliche Quellen bei nachrichtendienstlichen Gegenoperationen, die sich zum Schein einem ausländischen Nachrichtendienst verpflichtet haben, tatsächlich aber für die Schweizer Behörden tätig sind). Die Gefährdungslage dieser Personen lässt sich mit derjenigen von verdeckten Ermittlern vergleichen, die über einen weitreichenden Schutz verfügen. Von daher rechtfertigt es sich, auch für Informantinnen und Informanten Möglichkeiten zur Gewährung eines wirksamen Schutzes zu schaffen.

Die Schutzregelungen sind von der Kronzeugenregelung klar zu unterscheiden, die ursprünglich aus dem angloamerikanischen Strafprozessrecht stammt. Als Kronzeugen kommen dort Personen in Frage, die zwar grundsätzlich mitverantwortlich für die in Frage stehende Straftat scheinen, die jedoch unter Zusicherung von Straffreiheit, Strafreduktion oder anderer prozessualer Vorteile dafür gewonnen werden können, gegen Mitbeschuldigte als Zeuginnen auszusagen. Eine Expertenkommission des Bundes kam in ihrem Bericht «Vereinheitlichung des Strafprozessrechts»

zum Schluss, dass die Einführung der Kronzeugenregelung in der Schweiz auf strafprozessualer Ebene nicht angezeigt ist. Gleich verhält es sich auf präventiver Ebene. Eine Strafbefreiung im Sinne der erwähnten Kronzeugenregelung steht nicht zur Diskussion. Bei der Prävention liegt der Fokus nicht auf der Aufklärung von konkreten Straftaten, die mit besonderen Zeugenaussagen erleichtert werden soll, sondern auf dem Erhalt von Informationen, die für die Sicherheit bedeutsam sind; damit sollen Gefährdungslagen erkannt und entschärft und wenn möglich zukünftige Straftaten verhindert werden.

Im Übrigen dürfte die Massnahme nur in seltenen Ausnahmefällen mit zu erwartendem hochkarätigem Informationsgewinn angewendet werden. Zu denken ist etwa an den Schutz von Personen, die wichtige Informationen zur Verhinderung von erheblichen sicherheitspolitischen Risiken geben können, beispielsweise über Planung oder Vorbereitung von Terroranschlägen, konkrete Spionageaktivitäten gegen die Schweiz oder Strukturen zur Beschaffung von Massenvernichtungswaffen unter Missbrauch der Schweiz. Um die mit einer Kooperation einhergehende Gefährdung zu minimieren, würden hier nach der ersten Kontaktnahme Sondierungsgespräche erfolgen und bei gegebenen Voraussetzungen eine Schutzvereinbarung mit gegenseitigen Rechten und Pflichten verhandelt. Daran würde sich die Kooperation im eigentlichen Sinne anschliessen. Ein Schutz vor Strafverfolgung in der Schweiz wäre damit nicht verbunden.

Abs. 1

Mit der Bestimmung in diesem Absatz wird die rechtliche Grundlage für Massnahmen zum Schutz von Informantinnen und Informanten geschaffen. Bei den notwendigen Massnahmen, die das Bundesamt für Polizei treffen muss, um Leib und Leben dieser Personen zu schützen, handelt es sich um Personenschutzmassnahmen und örtliche Veränderungen. Unter Personenschutz sind Massnahmen zu verstehen wie der Einsatz von Leibwächtern, Schutzfahrzeugen oder -geräten oder bauliche Massnahmen. Die örtliche Veränderung kann in einem mit Zustimmung der betroffenen Person erfolgten Wechsel an einen anderen Aufenthaltsort im In- oder Ausland bestehen. Geeignete Schutzvorkehrungen zugunsten einer ins Ausland verbrachten Person bedeuten, dass eine Person, der auf Grund der Gesamtumstände trotz allem in der Schweiz kein geeigneter Schutz geboten werden kann, an einen sichereren Ort im Ausland gebracht wird. Um die damit verbundenen Umtriebe, eventuell auch einen Erwerbsausfall zu kompensieren, muss diese Massnahme mit einer befristeten finanziellen Unterstützung verbunden werden.

Das Bundesamt für Polizei kann die Schutzmassnahmen selbst treffen oder sie finanzieren. In der Praxis werden nur wenige solche Massnahmen notwendig sein und sich auch umsetzen lassen. Da sich aufgrund der Grösse der Schweiz hierzulande für bestimmte Gefährdungslagen kaum umfassende Schutzmassnahmen realisieren lassen, müssten in solchen Fällen ausländische Behörden eingeschaltet werden, womit auch die Kosten kalkulierbar sind. Denkbar ist auch die Gewährung von Teilschutzaspekten, beispielsweise die Zusicherung einer Aufenthaltsregelung (sei es in der Schweiz oder in einem befreundeten Drittstaat). Der zweite Satz von Artikel 1 weist ausdrücklich auf diese Möglichkeit hin.

Abs. 2

Aus denselben Überlegungen muss das Bundesamt für Polizei auch Schutzvorkehrungen zugunsten von Personen treffen können, die einer Informantin oder einem

Informanten nahe stehen, wenn deren Sicherheit von diesen Vorkehrungen abhängt. Mit der Kann-Formulierung wird sichergestellt, dass das Bundesamt für Polizei über den notwendigen Ermessensspielraum verfügt, um von Fall zu Fall die geeigneten Massnahmen treffen zu können.

Abs. 3

Diese Bestimmung sieht als Schutzmassnahme das Ausstatten mit einer Tarnidentität vor, die im Unterschied zu den in den Absätzen 1 und 2 genannten Massnahmen erst getroffen wird, wenn das Bundesamt für Polizei seine Kontakte zu einer Informantin oder einem Informanten beendet und die Informationsquelle nicht länger einsetzt. Ist die Sicherheit dieser Person wegen ihrer Zusammenarbeit mit dem Bundesamt für Polizei erheblich gefährdet, kann es diese Person mit einer bleibenden Tarnidentität ausstatten, um sie zu schützen. Die Person ist in der Folge berechtigt, diese Identität nach den Instruktionen des Bundesamts für Polizei zu benutzen. Voraussetzung für eine Tarnidentität ist die Zustimmung des Bundesverwaltungsgerichts und die Ermächtigung des Departementvorstehers oder der Departementsvorsteherin (vgl. unten).

Diese Bestimmung regelt aber nicht die Informationsbeschaffung unter Verwendung einer Tarnidentität: Die Informationsbeschaffung mithilfe einer Tarnidentität darf nur unter besonderen Bedingungen und nach dem dafür vorgesehenen besonderen Verfahren eingesetzt werden (siehe dazu die Erläuterungen zu Art. 14*d*).

Das Departement ist gemäss Artikel 27 Absatz 1bis des vorliegenden Entwurfs dazu verpflichtet, den Bundesrat und die parlamentarischen Kontrollstellen regelmässig über die Zahl der erstellten Tarnidentitäten, über den Zweck, zu dem sie erstellt worden sind, und über ihren konkreten Einsatz zu unterrichten. Dies gilt auch für Tarnidentitäten nach Absatz 3.

Abs. 4

Dieser Absatz bestimmt, dass Schutzvorkehrungen im Normalfall zeitlich zu befristen sind. Das Gesetz kann die Dauer indessen nicht abschliessend festlegen, da sie den Erfordernissen des Einzelfalles angepasst werden müssen. Ausnahmsweise kann der Departementsvorsteher oder die Departementsvorsteherin von einer zeitlichen Begrenzung absehen, wenn eine Person erkennbar auf Dauer besonders stark gefährdet ist; in einem solchen Fall können die Schutzvorkehrungen unbefristet gelten.

Art. 14d Tarnidentitäten

Nachrichtendienste und polizeiliche Präventionsbehörden sind zur Wahrnehmung ihrer Aufgaben und zum Schutz ihrer Mitarbeitenden bei der Beschaffung von Informationen in bestimmten Umfeldern auf die Nutzung von Tarnungen angewiesen. Die Schaffung solcher Tarnidentitäten ist dabei immer auf Dauer angelegt und kann selten erst mit der Aufnahme eines bestimmten Falles begonnen werden. Die Regelung der Tarnidentitäten gehört deshalb nicht in den Bereich der besonderen Mittel der Informationsbeschaffung, die an sehr restriktive Voraussetzungen gebunden ist (vgl. die Erläuterungen zu Abs. 1).

Der strategische Nachrichtendienst SND verfügt seit 1998 auf der Basis von Artikel 99 des Militärgesetzes über die Möglichkeit, seine Beschaffungsorgane mit Tarnidentitäten auszustatten (vgl. Jahresbericht 2002/2003 der Geschäftsprüfungskom-

missionen und der Geschäftsprüfungsdelegation vom 23. Januar 2004; BBl *2004* 1743). Die Kontrolle hierüber üben der Vorsteher oder die Vorsteherin des VBS und der Sicherheitsausschuss des Bundesrates aus.

Der Vorsteher oder die Vorsteherin des EJPD kann das Bundesamt für Polizei im Einzelfall ermächtigen, eine Tarnidentität zu schaffen. Vorab prüft das Bundesverwaltungsgericht (Genehmigungsverfahren nach Art. 18*d*), ob die Massnahme rechtsmässig ist, das heisst, ob die gesetzlichen Voraussetzungen dafür gegeben sind. Erst dann kann der Departementsvorsteher oder die Departementsvorsteherin seine bzw. ihre staatspolitische Beurteilung vornehmen und gegebenenfalls das Einverständnis erteilen.

Zu betonen bleibt, dass Tarnidentitäten im nachrichtendienstlichen Bereich ausschliesslich zu zwei Zwecken benutzt werden dürfen: Sicherheit für Mitarbeitende und Informationsbeschaffung. In allen übrigen Fällen ist ihr Einsatz unzulässig. Da nachrichtendienstliche Abklärungen nach BWIS und strafrechtliche Ermittlungen nicht deckungsgleich sind, sich vielmehr in Bezug auf das auslösende Ereignis, den Gegenstand der Abklärungen und dem damit verfolgten Ziel tiefgehend unterscheiden, kann auch nicht auf die Überwachungsmöglichkeiten gemäss Strafverfahrensrecht zurückgegriffen werden.

Abs. 1

Dieser Absatz schafft die Grundlage für den Einsatz von Tarnidentitäten zum Zweck der Informationsbeschaffung und zur Gewährleistung der Sicherheit von Beschaffungsorganen. Vorab sei darauf hingewiesen, dass die Verwendung von Tarnidentitäten sich meistens im Rahmen der allgemeinen Informationsbeschaffung bewegt, also für Massnahmen nach Artikel 14 Absatz 2 BWIS. Wenn hingegen bestimmte Massnahmen mit besonderen Mitteln der Informationsbeschaffung durchgeführt werden sollen, welche die Verwendung einer Tarnidentität erfordern (beispielsweise eine Observation an auch unter Verwendung einer Tarnidentität nicht allgemein zugänglichen Orten), so gelangt für die Anordnung dieser Massnahmen das Verfahren der besonderen Informationsbeschaffung nach den Artikeln 18*a* ff. zur Anwendung. Der Personenkreis, der mit einer Tarnidentität ausgestattet werden kann, wird in Absatz 1 abschliessend aufgezählt.

Buchstaben a und b: Die Sicherheitsorgane gemäss BWIS sind zwar eng an die schweizerischen Polizeikräfte gebunden und können den Grossteil ihrer Beschaffungstätigkeiten offen als Polizeiangehörige durchführen. Trotzdem ist es bei der Anbahnung von Kontakten zu Strukturen namentlich im Bereich des Terrorismus oder des verbotenen Nachrichtendienstes bisweilen nötig, dies unter Tarnung vornehmen zu können. Solche Massnahmen dienen nicht zuletzt auch dem Schutz der Mitarbeitenden der Sicherheitsorgane und ihrer Familien.

Buchstabe c: Auch Informantinnen und Informanten sollen mit Legenden ausgestattet werden können, wenn dies für die Nachrichtenbeschaffung unentbehrlich ist. Zu denken ist namentlich an Personen, die sich nur so in bestimmte staatsschutzrelevante Kreise einschleusen lassen, und die für ihren Schutz eine Tarnidentität benötigen. Informantinnen und Informanten werden zwar von den Führungsoffizieren der Sicherheitsorgane bezüglich der Informationsbeschaffung eng geführt, stehen aber nicht unter der direkten Dienstaufsicht der Sicherheitsorgane. Deshalb soll der Einsatz von Tarnidentitäten in diesen Fällen zeitlich und örtlich beschränkt und nur im Zusammenhang mit einer bestimmten Operation möglich sein.

Mit der Schaffung einer Tarnidentität ist auch das Recht verbunden, unter ihr Rechtsgeschäfte zu tätigen, namentlich Tarnstrukturen zu errichten. Personen mit einer Tarnidentität haben die volle Rechtspersönlichkeit und können Verträge schliessen (z.B. Anmieten von Lokalitäten und Fahrzeugen oder Fernmeldeanschlüssen, Schaffung von Tarnstrukturen wie Firmen oder andere juristische Personen).

Abs. 2

Eine Tarnidentität soll grundsätzlich solange aufrechterhalten werden können, wie es operativ erforderlich ist. Im Gegenzug ist darauf zu verzichten, sobald die damit verfolgten Ziele erreicht sind.

Um die Risiken besser kontrollieren zu können, die mit der Verwendung einer Tarnidentität verbunden sind, empfiehlt es sich, die Zeit zu begrenzen, während der eine Tarnidentität verwendet werden darf. Diese Vorkehrung ist besonders bei Informantinnen und Informanten angezeigt, die keine Angestellten des Bundesamts für Polizei sind und somit nicht dessen Disziplinargewalt unterstehen. Die Befristung der Ermächtigung ist demnach im Sinne eines «so lange wie nötig, längstens aber» zu verstehen. Besteht nach Ablauf der Befristung, gegebenenfalls deren Verlängerung, weiterhin Bedarf an einer Tarnidentität, ist neu Antrag zu stellen.

Abs. 3

Absatz 3 stellt sicher, dass eine Tarnidentität nur zu den vom BWIS verfolgten Zwecken gebraucht werden darf. Des Weiteren sei darauf hingewiesen, dass nach Artikel 27 Absatz 1bis Buchstabe a des vorliegenden Entwurfs das Ausstellen und die Verwendung der Tarnidentitäten Gegenstand einer gezielten, intensiven politischen Kontrolle sein soll, in deren Rahmen das Departement den Bundesrat und die Geschäftsprüfungsdelegation jährlich zu unterrichten hat.

Art. 15 Abs. 6

Die Bestimmung gründet auf der Regelung der früheren Bundespolizei, bei welcher Repression und Prävention vereint waren. Mit der Trennung von Repression und Prävention und deren organisatorischen Umsetzung wurde die Bestimmung obsolet. Nach heutigem Recht und Verständnis geht mit dem Informationsfluss von der Repression an die Prävention eine Zweckänderung einher; die Daten werden zu Daten präventiver Natur und sind nach dem in der Prävention anwendbaren Recht zu bearbeiten. Die Aufhebung bedeutet nicht, dass keine Daten mehr ausgetauscht werden könnten.

Art. 17 Abs. 3 Bst. e

Abs. 3 Bst. e

Beim sog. Clearing handelt es sich um eine seit langem wahrgenommene Aufgabe des DAP im Verkehr mit dem Ausland. Er führt auf Ersuchen eines ausländischen Dienstes eine Personensicherheitsprüfung über Schweizerinnen oder Schweizer oder dauerhaft in der Schweiz wohnhafte ausländische Personen durch um diesen die Mitarbeit an klassifizierten ausländischen Projekten (oder Anstellungen) zu ermöglichen. Für die Zusicherung des ersuchenden Staates, über das Einverständnis der betroffenen Person zur Vornahme des Clearings zu verfügen, wird neu ausdrücklich

die Schriftform festgelegt, wie dies von vielen Vernehmlassungsteilnehmerinnen und -teilnehmern gewünscht wurde.

Für die Vornahme der Clearings stützt sich der DAP seit jeher auf Artikel 17 Absatz 3 Buchstaben c BWIS. In der Vergangenheit wurde diese Rechtsgrundlage jedoch von verschiedener Seite in Frage gestellt. Deshalb soll nun eine formelle Gesetzesgrundlage für Clearings geschaffen werden. Dies ist notwendig, damit die Stellen im Bundesamt für Polizei, welche Clearings durchführen, im Rahmen des vom Bundesamt für Justiz vorbereiteten Gesetzgebungsprojekts zur Neuregelung der Zugriffsrechte des Bundesamts für Polizei auf VOSTRA (Datenbank für Strafregisterauszüge) mitberücksichtigt werden können. Denn für den Zugriff des Bundesamts für Polizei auf VOSTRA zum Zwecke des Clearings braucht es aus datenschutzrechtlicher Sicht zusätzlich eine klare Rechtsgrundlage in den Artikeln 365 ff. StGB. Die vorliegende BWIS-Änderung schafft somit die Grundlage, damit in Zukunft auch eine klare Regelung für den Zugriff auf Strafregisterdaten möglich wird. Die Strafregisterauszüge bilden für Clearings ein wichtiges Beurteilungselement. Ohne dieses würde das Clearing durch den DAP für das Ausland mit entsprechend negativen Auswirkungen auf die zu «clearende» Person an Wert verlieren. Sie würde möglicherweise auch bei positivem Ausgang des Clearings nicht mehr als genügend vertrauenswürdig gelten, um im Ausland an geheimen oder vertraulichen Projekten mitzuarbeiten.

Kapitel 3*a*: Besondere Informationsbeschaffung

Kapitel 3*a* enthält die entscheidenden Bestimmungen der Revision. Sie ermöglichen es den Sicherheitsorganen künftig, für die präventive Informationsbeschaffung besondere Mittel einzusetzen.

Der Titel des Kapitels entspricht dem Grundgedanken, die dieser Form der Informationsbeschaffung zugrunde liegt. Sie unterscheidet sich von der in Kapitel 3 geregelten Informationsbeschaffung mit den dort aufgelisteten allgemeinen Mitteln und erfolgt mit besonderen Mitteln, die nicht in allen Fällen und nur während begrenzter Zeit eingesetzt werden dürfen.

Das Kapitel 3*a* ist in zwei Abschnitte unterteilt. Der erste Abschnitt ist den allgemeinen Bestimmungen gewidmet, die den Einsatz der besonderen Informationsbeschaffung regeln; der zweite behandelt die dazu einsetzbaren besonderen Mittel.

Art. 18a Grundsatz

Abs. 1

Der Zweck der besonderen Informationsbeschaffung ist das Erkennen oder Abwehren einer konkreten Gefahr für die innere oder äussere Sicherheit der Schweiz. Dabei müssen die Sicherheitsorgane nach Artikel 18*b* des vorliegenden Entwurfs schon vor einem Einsatz von besonderen Mittel der Informationsbeschaffung einen Verdacht der Gefährdung der Sicherheit gegen eine bestimmte Person, Organisation oder Gruppierung begründen können (vgl. BGE *109* Ia 273, 288–289: «Die Überwachung darf nicht dazu dienen, einen Verdacht zu begründen»).

Die Gefährdungen, zu deren Abwehr die besonderen Mittel der Informationsbeschaffung eingesetzt werden können, sind Terrorismus, verbotener politischer

oder militärischer Nachrichtendienst, verbotener Handel mit Waffen oder radioaktiven Materialien sowie verbotener Technologietransfer. Auf die von verschiedenen Vernehmlassungsteilnehmerinnen und -teilnehmern geforderte Ausdehnung des Geltungsbereiches auf gewalttätigen Extremismus und wirtschaftlichen Nachrichtendienst bzw. organisierte Kriminalität wurde verzichtet. Nach Überzeugung des Bundesrates gilt es, im Bereich der Bekämpfung der organisierten Kriminalität vorerst die Resultate der Effizienzvorlage abzuwarten.

Abs. 2

Im Absatz 2 werden die Mittel der Besonderen Informationsbeschaffung abschliessend genannt, d.h. es können keine anderen Mittel zum Einsatz gelangen.

Art. 18b Voraussetzungen

Für den Einsatz der besonderen Mittel der Informationsbeschaffung müssen fünf Bedingungen kumulativ erfüllt werden.

Die ersten vier Bedingungen sind materieller Art; sie entsprechen den Anforderungen von Artikel 36 BV. Definiert werden zunächst das öffentliche Interesse und die Umstände, unter denen fallweise eine Einschränkung der Grundrechte gerechtfertigt ist (Bst. a). Des Weiteren wird den unterschiedlichen Aspekten des Grundsatzes der Verhältnismässigkeit Rechnung getragen (Bst. b–d).

Unter den Begriff des öffentlichen Interesses fallen die Wahrung der inneren und äusseren Sicherheit der Schweiz sowie der Schutz der Mitarbeiterinnen und Mitarbeiter des Bundesamts für Polizei vor Personen, Organisationen und Gruppierungen, die eine Gefährdung der inneren oder äusseren Sicherheit darstellen. Diese Personen, Organisationen und Gruppierungen werden als mutmassliche Gefährder bezeichnet; vgl. Buchstabe a.

Insbesondere der Schutzaspekt darf nicht unterschätzt werden: Die Mitarbeiterinnen und Mitarbeiter des Bundesamts für Polizei (einschliesslich menschliche Quellen) können – vor allem im Rahmen der operativen Informationsbeschaffung – einer stark erhöhten Gefährdung ausgesetzt sein. Bei ausgewiesenem Bedürfnis sollen deshalb zu ihrem Schutz Vorsichtsmassnahmen ergriffen werden dürfen. Regelmässig geht es darum, die betroffenen Personen im Einsatz zu begleiten und im Falle einer Gefährdung (z.B. Enttarnung) rechtzeitig in Sicherheit bringen zu können.

Beim Grundsatz der Verhältnismässigkeit gilt es – soweit möglich – zwischen den zugrunde liegenden Komponenten zu unterscheiden: Geeignetheit nach Buchstabe d in initio, wonach das Mittel, das zum Erfüllen des im öffentlichen Interesse verfolgten Zweckes eingesetzt wird, angemessen sein muss; Erforderlichkeit nach Buchstaben c und d in fine, wenn die herkömmlichen Mittel sich als unwirksam erwiesen haben; Verhältnismässigkeit im engeren Sinne in Buchstabe b, wenn das öffentliche Interesse überwiegt und somit einen Eingriff in die Rechte der betroffenen Person rechtfertigt.

Art. 18c Überwachung Dritter und Schutz des Berufsgeheimnisses

Abs. 1

Die Bestimmung in diesem Absatz regelt den Fall einer indirekten Implikation von Drittpersonen. Es ist denkbar, dass der mutmassliche Gefährder, der Ziel einer

Abklärung mit besonderen Mitteln der Informationsbeschaffung ist, Mittel oder Orte benutzt, die nicht ihm gehören, sondern einer Drittperson, beispielsweise ein fremder Telefonanschluss oder ein privates lokales Informationssystem. Dabei ist es durchaus möglich, dass diese Mittel und Orte ohne Wissen dieser Drittperson benutzt werden. Nichtsdestoweniger müssen diese Kommunikationsmittel und Orte bezüglich des Gefährders überwacht werden können.

In der Bestimmung kommt klar zum Ausdruck, dass die Drittperson nicht um ihretwillen überwacht wird, solange sie nicht selbst als mutmasslicher Gefährder oder mutmassliche Gefährderin betrachtet wird. Vielmehr ist es ihr Umfeld, das überwacht wird.

Abs. 2

Diese Bestimmung ist nicht auf Drittpersonen beschränkt, sondern regelt jegliche direkte oder indirekte Implikation einer an ein Berufsgeheimnis gebundenen Person. Der Zweck der Bestimmung ist die bestmögliche Wahrung des jeweiligen Berufsgeheimnisses. So gilt die Bestimmung sowohl für Dritte, deren Umfeld nach Massgabe des Absatzes 1 überwacht wird, wie auch für Personen, die Ziel einer Aufklärung mit besonderen Mitteln der Informationsbeschaffung sind. Der Text der Bestimmung lehnt sich an Artikel 4 Absatz 6 des Bundesgesetzes vom 6. Oktober 2000[46] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) an. In Übereinstimmung mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (Entscheid Kopp gegen die Schweizerische Eidgenossenschaft, 25. März 1998) muss die Triage der Überwachungsergebnisse von einer Gerichtsbehörde beaufsichtigt werden. Dieser auf ein Strafverfahren bezogene Entscheid kann auf die Prävention übertragen werden. Richtig erscheint deshalb, das Bundesverwaltungsgericht mit dieser Aufgabe zu betrauen (siehe auch die Botschaft zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung vom 1. Juli 1998; BBl *1998* 4241 4323).

Berufsgeheimnisträgerinnen – und träger nach Artikel 321 StGB sind Geistliche, Rechtsanwälte, Verteidiger, Notare, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Apotheker, Hebammen sowie ihre Hilfspersonen, für Tatsachen, die ihnen infolge ihres Berufs anvertraut wurden oder die sie bei dessen Ausübung wahrgenommen haben. Nicht unter Artikel 321 StGB fallen beispielsweise die Geheimnisträgerinnen und -träger nach Artikel 47 des Bankengesetzes vom 8. November 1934[47](BankG). Ein besonderer Schutz rechtfertigt sich hier – wie im Strafprozessrecht – nicht, weil der Einsatz von besonderen Mitteln der Informationsbeschaffung einerseits sowohl vom Bundesverwaltungsgericht, wie auch von der Vorsteherin oder vom Vorsteher des EJPD und des VBS genehmigt werden muss. Diese können allenfalls berechtigten Schutzinteressen Rechnung tragen. Andererseits wird die Bank nicht zur aktiven Auskunftserteilung angehalten (insofern wahrt sie das Bankkundengeheimnis); vorliegend geht es einzig um die Frage, ob eine Richterin oder ein Richter des Bundesverwaltungsgerichts die Triage der aus einer Überwachung erhobenen Daten beaufsichtigt. Hinzu kommt, dass Artikel 47 BankG u.a. alle Organe und Angestellten einer Bank zur Geheimhaltung verpflichtet; eine zahlenmässig derart umfassende Ausnahmeregelung würde keinen Sinn ergeben.

46 SR **780.1**
47 SR **952.0**

Art. 18d Genehmigungsverfahren

Durch den Einsatz von besonderen Mitteln der Informationsbeschaffung werden Grundrechte eingeschränkt, insbesondere das durch Artikel 8 der Europäischen Menschenrechtskonvention[48] (EMRK) und Artikel 13 BV gewährleistete Recht auf Achtung des Privatlebens. Zudem kann sich wegen des verdeckten Charakters der besonderen Informationsbeschaffung eine überwachte Person während der Dauer der Massnahme nicht dagegen wehren. Umso wichtiger ist es deshalb, dass die Anwendung der einschlägigen Gesetzesbestimmungen möglichst präzise geregelt ist und streng kontrolliert wird, ob sie eingehalten werden.

Die Kontrolle erfolgt doppelt und gestaffelt. Personen, gegen die besondere Mittel der Informationsbeschaffung eingesetzt wurden, müssen nach Beendigung des Einsatzes über diese Massnahme unterrichtet werden; sie können dagegen beim Bundesverwaltungsgericht Beschwerde einlegen (nachträgliche Prüfung). Die Pflicht zur nachträglichen Mitteilung von Mitteln der besonderen Informationsbeschaffung an die betroffenen Personen und die Orientierung über die Beschwerdemöglichkeit werden in den Artikeln 18*i* (Mitteilungspflicht) und 29*a* (Rechtsschutz) geregelt.

Doch damit ist es nicht getan: Zum Zeitpunkt der nachträglichen Mitteilung sind ja bereits Grundrechte eingeschränkt worden. Zudem sieht das Gesetz vor, dass unter bestimmten Bedingungen von der Mitteilung (vorübergehend oder ganz) abgesehen werden kann (vgl. Art. 18*i* Abs. 2 des vorliegenden Entwurfs). Die nachträgliche Prüfung muss deshalb durch eine vorgängige Kontrolle so ergänzt werden, dass bereits zum Zeitpunkt, in dem der Einsatz von besonderen Mitteln der Informationsbeschaffung beantragt wird, eine vergleichbar strenge Überprüfung wie in einem Beschwerdeverfahren stattfindet.

Bei Massnahmen im Rahmen des Strafverfahrens schreibt das Gesetz in der Regel nach der Anordnung die Überprüfung durch eine richterliche Instanz vor. Da es sich um ähnliche Eingriffe in Grundrechte handelt, gibt es keinen Grund, für den Einsatz der besonderen Informationsbeschaffung zu präventiven Zwecken, auf die richterliche Prüfung zu verzichten. Im Grundsatzentscheid aus dem Jahr 1983 (BGE *109* Ia 295) hält das Bundesgericht fest, «dass Missbräuche … im präventiven Bereich noch weit mehr als bei der repressiven Überwachung schädliche Folgen für die freiheitliche demokratische Ordnung haben können». Dabei stellt sich die Frage, ob die vorgängige Prüfung einer geplanten Präventivmassnahme einer Gerichtsinstanz vorbehalten bleiben muss, oder ob eine gerichtsinstanzähnliche Stelle damit betraut werden kann, wobei die Mindestanforderung darin besteht, dass sie verwaltungsunabhängig ist.

Die Antwort des Europäischen Gerichtshofs für Menschenrechte (EGMR) und jene des Bundesgerichts auf diese Frage sind nicht ganz deckungsgleich: In der ständigen Praxis des EGMR reicht eine gerichtsinstanzähnliche Stelle. Das Bundesgericht scheint eine Prüfung durch eine formelle Gerichtsinstanz zu bevorzugen.

Im Entscheid Klass gegen die Bundesrepublik Deutschland vom 6. September 1978 befand der EGMR, dass hinsichtlich der präventiven Überwachung das deutsche Gesetz den Anforderungen des Artikels 8 Absatz 2 EMRK genügt. Darin ist vorgesehen, dass Telefonüberwachungen vorgängig von einem unabhängigen Komitee, bestehend aus drei von einer Bundestagskommission gewählten Mitgliedern, bewil-

48 SR **0.101**

ligt werden müssen. Voraussetzung ist, dass das Gesetz dann erlaubt, in die Privatsphäre von Personen einzugreifen, wenn der Eingriff im öffentlichen Interesse gerechtfertigt ist (beispielsweise wegen der nationalen oder öffentlichen Sicherheit), sich in einer demokratischen Gesellschaft als notwendig erweist (vgl. insbesondere § 21, 53 und 60 des Entscheids) und es der Zweck vor dem Hintergrund des Artikels 13 EMRK rechtfertigt (Recht auf wirksame Beschwerde).

Der Gerichtshof bemerkte zwar, dass es an sich wünschenswert wäre, dass in einem Bereich, in dem im Einzelfall zum Nachteil einer demokratischen Gesellschaft grosser Missbrauch betrieben werden könnte, die Prüfung von einem Richter vorgenommen werden würde. Er kam aber zum Schluss, dass mit dem deutschen System eines unabhängigen, wenngleich nicht richterlichen Komitees der Rahmen dessen, was in einer demokratischen Gesellschaft als notwendig gelten kann, nicht gesprengt werde (aaO, § 56).

Neuere Erwägungen des Bundesgerichts (in BGE *109* Ia 273 ff) legen diejenigen des EGMR etwas anders aus. Es war zu klären, ob ein Gesetz des Kantons Basel-Stadt über die Überwachung zu präventiven und repressiven Zwecken vor Artikel 8 EMRK und Artikel 36 Absatz 4 der damals gültigen Bundesverfassung (Garantie des Briefgeheimnisses) standhielt. «Bei der Beurteilung dieses Verfahrens ist insbesondere in Betracht zu ziehen, dass eine richterliche Behörde die Überwachung genehmigen muss. … Diese weitgehende obligatorische Kontrolle durch eine richterliche Behörde bietet dem Betroffenen … einen hinreichenden Schutz» (BGE *109* Ia 273, 296). Unter Verweis auf diesen Entscheid bekräftigt das Bundesgericht zwölf Jahre später: «die Telefonüberwachung als geheim durchgeführte Massnahme … bedarf einer richterlichen Prüfung» (BGE *122* I 182, 190, T., vom 2. Mai 1996). Im zweiten Fall stand allerdings die Anwendung der Überwachungsmassnahmen in förmlichen Strafverfahren zur Diskussion.

Unklar bleibt indessen, ob sich das Bundesgericht darauf beschränkte, das Gesetz des Kantons Basel-Stadt zu beschreiben und zum Schluss kam, es sei völlig EMRK- und verfassungskonform oder ob das Bundesgericht implizit ausdrücken wollte, dass die Bundesverfassung die Einschaltung eines Richters oder einer Richterin verlangt, auch wenn die EMRK dies nicht erfordert (vgl. Entscheid Klass). Anders ausgedrückt: Aus der Rechtssprechung des Bundesgerichts ist nicht sicher zu schliessen, ob es mit dem Europäischen Gerichtshof eine gerichtliche Instanz als wünschenswert, aber nicht zwingend, oder gestützt auf die Bundesverfassung – strenger als die EMRK – als obligatorisch erachtet.

Angesichts dieser Unklarheit gibt der Bundesrat im Zuge dieses Gesetzesentwurfs der Genehmigung durch eine gerichtliche Instanz den Vorzug.

Da aber der präventive Bereich eine im Rahmen des Gesetzes politisch gesteuerte, kontrollierte und verantwortete Tätigkeit ist, sieht der Entwurf ein doppeltes Kontrollverfahren mit einer zusätzlichen politischen Komponente vor. Es wird mit einem begründeten schriftlichen Antrag des Bundesamts für Polizei eingeleitet. Gestützt darauf beurteilt das Bundesverwaltungsgericht die beantragten Massnahmen (Genehmigungsverfahren). Nur soweit das Bundesverwaltungsgericht die Massnahmen genehmigt hat, prüft sie sodann der Vorsteher oder die Vorsteherin des EJPD, konsultiert den Vorsteher oder die Vorsteherin des VBS und entscheidet im Falle beidseitiger Zustimmung definitiv über den Vollzug der Massnahme (Anordnungsverfahren). Der Antrag wird also sowohl von der Judikative einer richterlichen Prüfung als auch von der Exekutive einer (nochmals doppelten) Prüfung nach

staatspolitischen Gesichtspunkten unterzogen. Nur wenn und soweit alle zustimmen, ist der Einsatz von besonderen Mitteln der Informationsbeschaffung zulässig.

Dieses gegenüber der Vernehmlassung gestraffte und bereinigte Verfahren trägt den Äusserungen zahlreicher Vernehmlassungsteilnehmerinnen und -teilnehmer Rechnung, welche zwar die doppelte Prüfung befürworteten, aber das in der Vernehmlassung vorgeschlagene Verfahren als zu unübersichtlich beurteilten.

Angesichts der auf dem Spiel stehenden Interessen und Rechtsgüter wird sodann auch ohne spezielle gesetzliche Grundlage davon ausgegangen, dass die zuständigen Richterinnen und Richter den Geheimhaltungserfordernissen bei der Behandlung der Fälle angemessen Rechnung tragen, weshalb auf den entsprechenden, im Vernehmlassungsentwurf noch enthaltenen, Absatz verzichtet wurde.

Abs. 4

Aufgabe des Bundesverwaltungsgerichts ist die Prüfung, ob bei der Schaffung von Tarnidentitäten die gesetzlichen Vorgaben eingehalten werden (vgl. Art. 14*c* Abs. 3, 4 und 14*d*). Dabei geht es um eine Rechtskontrolle, d.h. das Gericht hat sich über das Vorhandensein der in Artikel 14*c* Absatz 3 und 14*d*, Absatz 1 und 2 vorgesehenen Bedingungen zu vergewissern. Im Gegenzug spricht es sich nicht über die Opportunität der Schaffung solcher Tarnidentitäten aus; diese Befugnis steht dem Vorsteher oder der Vorsteherin des EJPD zu. Auch für die Tarnidentitäten ist die Zustimmung des Bundesverwaltungsgerichts also zwingender Natur (vgl. Art. 14*c* Abs. 3 und 14*d* Abs. 1). Die Entscheide des Bundesverwaltungsgerichts in diesem Bereich sind abschliessend.

Art. 18e Anordnungsverfahren

Abs. 1

An das Genehmigungsverfahren nach Artikel 18*d* schliesst sich das Anordnungsverfahren nach Artikel 18*e* an. Das Bundesamt für Polizei kann dem Departement nur dann den Einsatz von besonderen Mitteln der Informationsbeschaffung beantragen, wenn das Bundesverwaltungsgericht vorgängig der Massnahme zugestimmt hat. Auf Wunsch zahlreicher Vernehmlassungsteilnehmerinnen und -teilnehmer wird gleichzeitig ausdrücklich festgehalten, dass sich die Anordnung stets im vom Bundesverwaltungsgericht vorgegebenen Rahmen bewegen muss («im Rahmen des Entscheides des Bundesverwaltungsgerichts»); der entsprechende Entscheid ist deshalb dem Antrag beizulegen.

Der letzte Satz von Absatz 1 legt fest, dass das Bundesamt für Polizei das Departement über vom Bundesverwaltungsgericht abgelehnte Anträge unterrichtet. Mit diesem Vorgehen soll der Departementsleitung eine umfassende Sicht über die vom Bundesamt für Polizei gestellten Anträge (und nicht nur über die vom Bundesverwaltungsgericht genehmigten) ermöglicht werden.

Abs. 2 und 3

Der Vorsteher oder die Vorsteherin des EJPD konsultiert den Vorsteher oder die Vorsteherin des VBS und befindet – bei beidseitiger Zustimmung – abschliessend über den Vollzug der vom Bundesverwaltungsgericht genehmigten besonderen Mittel der Informationsbeschaffung; eine Delegation des Entscheides ist nicht möglich. Können sich die Vorsteher oder Vorsteherinnen des EJPD und des VBS über den beantragten und vom Bundesverwaltungsgericht genehmigten Einsatz von

besonderen Mitteln der Informationsbeschaffung nicht einigen, ist eine Vollzugsanordnung nicht zulässig.

Ungeachtet eines der beantragten Massnahme zustimmenden Entscheids des Bundesverwaltungsgerichts können der Vorsteher oder die Vorsteherin des EJPD bzw. des VBS im beidseitigen Einverständnis ganz oder teilweise auf den Vollzug der Massnahme verzichten oder den Vollzug mit zusätzlichen Einschränkungen oder Auflagen versehen (so beispielsweise eine regelmässige Orientierung über den Vollzug der Massnahme).

Je nach Fall kann der Departementsvorsteher oder die Departementsvorsteherin EJPD für die Entscheidfindung weitere Departementsvorsteherinnen oder Departementsvorsteher (etwa des EDA bei aussenpolitischen Interessen) konsultieren.

Art. 18f Dringlichkeitsverfahren

Artikel 18*f* sieht ein besonderes Verfahren für den Fall vor, dass Gefahr im Verzug ist. Wenn der Erfolg von Mitteln der besonderen Informationsbeschaffung durch ein Abwarten des Entscheids des Bundesverwaltungsgerichts oder des Vorstehers oder der Vorsteherin des EJPD bzw. des VBS gefährdet oder verunmöglicht würde, soll rasch gehandelt werden können. Dies ist etwa dann der Fall, wenn eine wichtige Zielperson überraschend in die Schweiz einreist und ab der Einreise intensiv – beispielsweise auch durch Überwachung des Fernmeldeverkehrs – überwacht werden muss.

Abs. 1

Die besonderen Mittel der Informationsbeschaffung werden in Dringlichkeitsfällen vom Direktor oder der Direktorin des Bundesamts für Polizei unmittelbar angeordnet und können sofort vollzogen werden. Auch in solch dringlichen Fällen müssen die materiellen Voraussetzungen nach Artikel 18*b* des Gesetzesentwurfs für den Einsatz besonderer Mittel vollumfänglich erfüllt sein. Es obliegt dem Direktor oder der Direktorin des Bundesamts für Polizei, sich über das Vorhandensein der Anordnungsvoraussetzungen zu vergewissern. Die Orientierung des Departementsvorstehers oder der Departementsvorsteherin erfolgt zeitgleich.

Abs. 2

Der Direktor oder die Direktorin des Bundesamts für Polizei ist verpflichtet, dem Bundesverwaltungsgericht den üblichen Antrag innert 24 Stunden nachzureichen, wobei die Dringlichkeit zu begründen ist. Alsdann nimmt das Verfahren seinen normalen Lauf. Das Bundesverwaltungsgericht hat seinen Entscheid dem Bundesamt für Polizei (wie beim «normalen» Verfahren) innert 72 Stunden mitzuteilen.

Abs. 3

Der Antrag des Bundesamts für Polizei für eine nachträgliche Anordnung des Einsatzes von besonderen Mitteln der Informationsbeschaffung bzw. für den weiteren Vollzug erfolgt im Rahmen des Entscheides des Bundesverwaltungsgerichts über die Rechtmässigkeit. Die Antragsstellung hat umgehend zu erfolgen. Voraussetzung für eine Vollzugsanordnung ist auch hier das beiderseitige Einverständnis der Vorsteherin oder des Vorstehers des EJPD bzw. des VBS.

Abs. 4

Lehnt das Bundesverwaltungsgericht den Antrag ab oder ordnet der Vorsteher oder die Vorsteherin des EJPD nach Konsultation der Vorsteherin oder des Vorstehers des VBS den weiteren Vollzug nicht innert 48 Stunden an, muss das Bundesamt für Polizei den Vollzug einstellen und sämtliche aus dieser Informationsbeschaffung stammenden und bis dahin erhobenen Daten unverzüglich vernichten (vgl. die analoge Bestimmung von Art. 7 Abs. 4 BÜPF).

Hat das Bundesamt für Polizei aus einer verweigerten Massnahme gewonnene Erkenntnisse bereits an andere Organe oder Behörden weitergegeben, muss es diese auffordern, sämtliche Aufzeichnungen über diese Erkenntnisse zu vernichten.

In diesem Zusammenhang wurde im Vernehmlassungsverfahren auf die Problematik hingewiesen, wie im Falle einer negativen Stellungnahme die Vernichtung von allenfalls bereits ins Ausland gelangten Daten sichergestellt werden könne.

Dazu Folgendes: Bei Dringlichkeitsverfahren ist im Regelfall davon auszugehen, dass auch allfällige Datenweitergaben an ausländische Partnerdienste rasch (d.h. innert Stunden) erfolgen müssen (z.B. über die weiteren Reisepläne einer Zielperson); Raum für vorgelagerte gerichtliche Verfahren (z.B. superprovisorische Verfügungen) besteht deshalb keiner. Schon nach geltendem Recht dürfen ausländische Partnerdienste erhaltene Informationen nur für den Zweck, zu welchem sie weitergegeben wurden, verwenden, und der DAP kann Auskunft über deren Verwendung verlangen. Das beinhaltet auch die Orientierung der jeweiligen ausländischen Behörde über die Berichtigung oder die Vernichtung von Daten. Es ist zwar ausgeschlossen, dass sich Schweizer Amtsstellen bei ausländischen Nachrichtendiensten oder Sicherheitsbehörden über eine tatsächliche Vernichtung oder die Verwendung von Daten vergewissern können. Es ist dennoch davon auszugehen, dass im Falle einer verweigerten Genehmigung die ins Ausland gelangten Daten auf entsprechende Aufforderung des DAP hin vernichtet werden: Zum einen hat weder ein schweizerischer noch ein ausländischer Nachrichtendienst Interesse an als falsch oder unzulässig erklärten Daten. Zum anderen erfolgt die Informationsweitergabe an das Ausland standardmässig mit dem Vorbehalt, dass die übermittelte Information ohne ausdrückliche Zustimmung des DAP nicht weitergegeben werden darf (sog. «Drittdienstregel»). Selbstredend würde bei gegebener Sachlage eine solche Zustimmung vom DAP verweigert, womit sich die Daten für den fraglichen ausländischen Dienst de facto als wertlos erweisen würden. Schliesslich sei darauf hingewiesen, dass der Informationsaustausch mit ausländischen Diensten – anders als im Rechtshilfeverfahren – auf freiwilliger Basis erfolgt. Hält sich ein ausländischer Partnerdienst nicht an die Regeln, kann die Schweiz die weitere Zusammenarbeit jederzeit einstellen oder einschränken.

Art. 18g Einstellung des Einsatzes

Wird die Informationsbeschaffung nicht mehr benötigt (Bst. a), ist sie aussichtslos (Bst. b), wird sie nicht verlängert (Bst. c) oder wird sie, im Falle eines dringlichen Verfahrens, vom Bundesverwaltungsgericht als nicht rechtmässig beurteilt oder vom Vorsteher oder der Vorsteherin des EJPD, nach Konsultation des Vorstehers oder der Vorsteherin des VBS, abgelehnt oder nicht innert 48 Stunden angeordnet (Bst. d und e), so stellt sie das Bundesamt für Polizei umgehend ein. Dabei kann das Verhältnismässigkeitsprinzip gebieten, dass nicht nur ganze Einsätze, sondern schon einzelne Teile bei Andauern des Einsatzes selber eingestellt werden.

Art. 18h Bearbeiten der mit besonderen Mitteln beschafften Personendaten

Abs. 1

Diese Bestimmung regelt die Rahmenbedingungen für die Aufbewahrung der in Artikel 15 BWIS aufgelisteten Daten. Die gesammelten Daten müssen innerhalb von dreissig Tagen nach Beendigung des Einsatzes vernichtet werden, wenn sie keinen Bezug zur Gefährdung aufweisen, wegen der die besonderen Mittel der Informationsbeschaffung angeordnet wurden.

Den in der Vernehmlassung vereinzelt geäusserten Anliegen, die Informationstriage sei nicht vom Bundesamt für Polizei selber vorzunehmen oder zumindest vom Bundesverwaltungsgericht zu kontrollieren, kann aus praktischen und rechtlichen Überlegungen nicht entsprochen werden: Einerseits setzt die erforderliche Triage umfassende Fallkenntnisse voraus, die sich Aussenstehende mit vertretbarem Aufwand innert nützlicher Frist kaum aneignen können. Anderseits wird die Arbeit des Bundesamts für Polizei ohnehin bereits von verschiedenen Stellen streng kontrolliert (departementsinternes Inspektorat, parlamentarische Aufsicht usw.), weshalb keine Notwendigkeit für ein zusätzliches, neu zu schaffendes Kontrollinstrument besteht.

Art. 18i Mitteilungspflicht

Diese Bestimmung ist ein zentrales Element des Gesetzesentwurfs und massgeblich für die Ausgestaltung der nachträglichen Prüfung. Erst mit der Information wird den betroffenen Personen ermöglicht, ihr Beschwerderecht nach Artikel 29*a* vor Gericht wahrzunehmen.

Die Pflicht, Betroffene zu informieren, ist verfassungsrechtlicher Natur und ergibt sich implizit aus der Garantie der Achtung des Privatlebens einer Person und ihres Briefverkehrs. Diese Garantie gründet in Artikel 8 EMRK und Artikel 13 BV. Gemäss Bundesgerichtsentscheid *109* Ia 273, 298–299, hat dies für die präventive und die repressive Überwachung sowie gegenüber den Angeschuldigten und Verdächtigten und Drittpersonen zu gelten. …». Demnach ist grundsätzlich von der Pflicht auszugehen, Überwachungsmassnahmen den Betroffenen bekannt zu geben.

Unterrichtet das Bundesamt nach Abschluss eines Einsatzes die betroffene Person ausnahmsweise nicht darüber, dass über sie mit besonderen Mitteln Informationen gesammelt wurde, hat die betroffene Person in der Regel keine Möglichkeit, sich nachträglich dagegen zu wehren, es sei denn, sie habe auf anderem Weg davon erfahren. Für solche Fälle muss deshalb wie im Strafverfahren ein zusätzliches richterliches Verfahren die Rechtmässigkeit garantieren.

Abs. 1

In Befolgung dieser Rechtsprechung verankert der vorliegende Gesetzesentwurf den Grundsatz der nachträglichen Mitteilungspflicht. Ist eine Operation beendet, muss das Bundesamt für Polizei Betroffene grundsätzlich binnen Monatsfrist über die Informationsbeschaffung unterrichten (zum Begriff der Operation siehe Art. 14 VWIS).

Eine Ausdehnung der Mitteilungspflicht auf die allgemeine Informationsbeschaffung oder auf alle von der Überwachung erfassten Personen, wie dies einzelne Vernehmlassungsteilnehmerinnen und -teilnehmer wünschten, ist weder gerechtfertigt noch praktikabel: Einerseits wird mit der allgemeinen Informationsbeschaffung bloss marginal in Grundrechte eingegriffen. Anderseits wäre die Folge ein riesiger

Verwaltungsaufwand, gälte es doch nicht nur, jährlich Tausende von Abklärungen anzuzeigen (und diese selbst dann, wenn sie ergebnislos endeten), sondern ebenso, ein Mehrfaches davon an Personen zu identifizieren (nämlich nicht nur die Betroffenen, sondern auch zufällig Anwesende). Ebenso wenig besteht Anlass, zufällig betroffenen Drittpersonen von Überwachungen oder hängigen Verfahren gegen die Zielperson Kenntnis zu geben.

Abs. 2 und 3

Im erwähnten Entscheid Klass (§§ 57 bis 59, siehe Kommentar zu Art. 18*d*) stellte der EGMR fest, dass eine nachträgliche Mitteilung sehr wohl den langfristigen Zweck einer Überwachung in Frage stellen könne. Ausserdem bestehe die Gefahr, dass die Arbeitsmethoden von Nachrichtendiensten, die überwachten Bereiche und gegebenenfalls sogar die Identität von Ermittelnden preisgegeben werden. Deshalb wurden die Ausnahmen, die das deutsche Gesetz für die Mitteilungspflicht vorsieht, für rechtmässig befunden.

In seinem Entscheid aus dem Jahr 1983 folgte das Bundesgericht diesen Erwägungen (BGE *109* Ia 273, 300–301) und anerkannte nahezu die gleichen Ausnahmen. Es hielt dafür, dass «diese Ausnahmen … allerdings streng anzuwenden» seien. In der Praxis wird – ungeachtet dieses mahnenden Vorbehaltes – die Mitteilungspflicht durch die Erfordernisse des Strafverfahrens relativiert. Die in Absatz 2 Buchstaben a–d aufgeführten Ausnahmen sind weitgehend Artikel 10 Absatz 3 BÜPF und Artikel 22 Absatz 2 des Bundesgesetzes vom 20. Juni 2003[49] über die verdeckte Ermittlung nachgebildet. Die Aufzählung in den Buchstaben a–d ist abschliessend.

Nicht erreichbar (Bst. d) ist eine Person beispielsweise auch dann, wenn ihr Aufenthaltsort nur mit unverhältnismässigem Aufwand in Erfahrung gebracht werden kann oder dieser zwar bekannt ist, sie aber dort nur mit unverhältnismässigem Aufwand erreicht werden kann (namentlich im Ausland).

Im Übrigen liegt es nicht in der Kompetenz des Bundesamts für Polizei, die Mitteilung aufzuschieben oder ganz davon abzusehen. Da ein verfassungsmässiges Recht eingeschränkt wird, muss verfahrensmässig sichergestellt werden, dass das Individualinteresse des oder der Einzelnen, sich gegen Eingriffe in die Privatsphäre wehren zu können, nur dann beschränkt werden kann, wenn ein vorrangiges öffentliches Interesse einen Aufschub oder Verzicht der Mitteilung klar notwendig macht. Dieses Abwägen der gegenseitigen Interessen ist umso heikler, als das Mitteilungsverfahren auch die Möglichkeit vorsieht, bei einer richterlichen Behörde die Rechtmässigkeit des Einsatzes von Mitteln der besonderen Informationsbeschaffung überprüfen zu lassen. Es rechtfertigt sich deshalb, für das Verweigern oder Aufschieben der Mitteilungspflicht strenge Regeln vorzusehen: Gegebenenfalls stellt das Bundesamt für Polizei begründeten Antrag, warum von einer Mitteilung abgesehen werden soll. Anschliessend findet eine richterliche Prüfung durch das Bundesverwaltungsgericht statt. Entscheidet dieses für die Rechtmässigkeit der Verweigerung der Mitteilung, konsultiert der Vorsteher oder die Vorsteherin des EJPD den Vorsteher oder die Vorsteherin des VBS nach Artikel 18*e* und entscheidet. Es gelangt mit anderen Worten dasselbe Verfahren wie bei der Anordnung von Mitteln der besonderen Informationsbeschaffung zur Anwendung.

49 SR **312.8**

Von der nachträglichen Mitteilungspflicht zu unterscheiden ist das Recht auf Auskunft im Sinne von Artikels 8–10 DSG. Dieses richtet sich nach Artikel 18 BWIS (sog. indirektes Auskunftsrecht). Gemäss dieser Bestimmung kann jede Person beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) verlangen, dass er prüfe, ob im Informationssystem des Bundesamts für Polizei rechtmässig Daten über sie bearbeitet werden. Der EDÖB teilt der gesuchstellenden Person in einer stets gleichlautenden Antwort mit, dass in Bezug auf sie entweder keine Daten unrechtmässig bearbeitet würden oder dass er bei Vorhandensein allfälliger Fehler in der Datenbearbeitung eine Empfehlung zu deren Behebung an das Bundesamt für Polizei gerichtet habe.

Anders als bei der nachträglichen Mitteilung, die eine Massnahme der besonderen Informationsbeschaffung voraussetzt, kann das indirekte Auskunftsrecht voraussetzungslos ausgeübt werden. Jede Person kann somit jederzeit durch den EDÖB den ordnungsgemässen Umgang mit seinen Daten überprüfen lassen. Die Mitteilung des EDÖB ihrerseits oder der Vollzug der von ihm abgegebenen Empfehlung wird auf Verlangen der betroffenen Person vom Präsidenten oder der Präsidentin der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts überprüft.

Diese jederzeitige Überprüfungsmöglichkeit der Datenbearbeitung durch den DAP setzt ein hohes Kontrollniveau um, findet ihre Rechtfertigung aber im Umstand, dass der betroffenen Person im Regelfall keine Akteneinsicht gewährt wird. Mit dieser Lösung wird einerseits sichergestellt, dass die Interessen der betroffenen Person vollumfänglich und fachkundig wahrgenommen werden, und anderseits verhindert wird, dass sich eine möglicherweise gefährliche Personen über gegen sie hängige oder getätigte Abklärungen ins Bild setzen kann.

Hinzu kommt, dass unter den bestimmten Voraussetzungen vom indirekten Auskunftsrecht abgewichen werden kann: Der EDÖB kann ausnahmsweise nach den Bestimmungen des DSG der gesuchstellenden Person in angemessener Weise Auskunft erteilen, wenn damit keine Gefährdung der inneren oder äusseren Sicherheit verbunden ist und wenn der gesuchstellenden Person sonst ein erheblicher, nicht wieder gut zu machender Schaden erwächst.

In diesem Zusammenhang wurde von verschiedenen Vernehmlassungsteilnehmerinnen und -teilnehmern auf einen Entscheid der früher zuständigen Eidgenössischen Datenschutz- und Öffentlichkeitskommission vom 15. Februar 2006 verwiesen. Dieser Entscheid wird gleich wie die übrige Rechtssprechung (z.B. zur EMRK) laufend analysiert. Insbesondere wird überprüft, inwieweit die Regelungen des BWIS, des Militärgesetzes und des Bundesgesetzes über polizeiliche Informationssysteme des Bundes (BPI) zu harmonisieren sind. Das BPI befindet sich bereits in parlamentarischer Beratung. Soweit notwendig wird das Departement bei der parlamentarischen Beratung der vorliegenden Revision die Problematik thematisieren und Lösungsvorschläge aufzeigen.

Art. 18j Vollzug durch die Kantone

Dieser Artikel besagt, dass für die im Auftrag des Bundes von den Sicherheitsorganen der Kantone mit besonderen Mitteln durchgeführte Informationsbeschaffung die Bestimmungen des BWIS gelten. Das heisst, wenn Sicherheitsorgane der Kantone im Auftrag des Bundes nicht allgemein zugängliche Orte überwachen oder dort Überwachungsgeräte installieren, sind die Bestimmungen der Artikel 18*a*–18*i* dieses

Gesetzesentwurfes massgebend und nicht allfällige Bestimmungen des kantonalen Rechts.

Wie sich das neue Instrumentarium auf die Kantone auswirkt, ist stark abhängig von Art und Ausgestaltung der einzelnen Massnahmen, vor allem aber von der (ereignisabhängigen) Notwendigkeit derer Nutzung. Je nach Betroffenheit werden die Kantone deshalb allenfalls zusätzliche personelle Mittel für die kantonalen BWIS-Vollzugsstellen (vgl. Art. 6 BWIS) einsetzen, für die sie vom Bund angemessen entschädigt werden (Art. 28 BWIS).

2. Abschnitt: Besondere Mittel der Informationsbeschaffung

Gemäss den Artikeln 36 Absatz 1 und 164 Absatz 1 Buchstabe a BV müssen schwerwiegende Einschränkungen der Grundrechte im Gesetz vorgesehen sein. Es genügt indessen nicht, die verschiedenen die Grundrechte möglicherweise einschränkenden Mittel lediglich aufzulisten. Vielmehr gilt es, im Einzelnen das Ausmass der Einschränkungen darzulegen, darauf hinzuweisen, worauf sie sich erstrecken, und wichtige Einzelheiten der zulässigen Handlungen zu regeln.

Im Übrigen wurde bereits darauf hingewiesen, dass die präventive Zweckausrichtung der Informationsbeschaffung einer Weitergabe an in- und ausländische Strafverfolgungsbehörden nicht entgegensteht (nach Art. 17 Abs. 1 BWIS besteht gegenüber inländischen Strafverfolgungsbehörden vielmehr eine Pflicht zur Weitergabe strafverfolgungsrelevanter Informationen). Dabei können nachrichtendienstliche Erkenntnisse («Intelligence») in vielfältiger Weise in ein Strafverfahren einfliessen, so beispielsweise im Rahmen der Analysetätigkeit oder durch Amtsberichte, und damit u.a. auch den zielgerichteten Einsatz der Ressourcen der Strafverfolgung ermöglichen.

Art. 18k Überwachen des Post- und Fernmeldeverkehrs

Die Überwachung des Post- und Fernmeldeverkehrs zu Zwecken der Strafverfolgung wird BÜPF) geregelt. Demgegenüber erfolgt das hier zu regelnde präventive Überwachen nicht zum Zweck der Strafverfolgung, sondern zur Erkennung von konkreten sicherheitspolitischen Gefährdungen durch Terrorismus, verbotenen politischen und militärischen Nachrichtendienst und verbotenen Handel mit Waffen und radioaktiven Materialien sowie durch verbotenen Technologietransfer. Eine besondere Regelung im BWIS ist deshalb angezeigt.

Das BWIS soll aber nur besondere Regeln aufstellen, wo Abweichungen oder Präzisierungen zum BÜPF notwendig sind. Für technische und organisatorische Fragen verweist es auf das BÜPF, weil nicht beabsichtigt ist, für die präventiven Überwachungen grundsätzlich andere Verfahren und technische Anforderungen zu definieren.

Nach dem klaren Wortlaut von Artikel 18i Absatz 1 des vorliegenden Gesetzesentwurfs sind andere am Verfahren beteiligte Behörden, wie beispielsweise der Dienst für Besondere Aufgaben (DBA) des UVEK, weder gehalten noch berechtigt, Auskunft über die Durchführung von auf das BWIS gestützte Überwachungsmassnahmen zu erteilen.

Abs. 1

In diesem Absatz wird der Zweck der Post- und Fernmeldeüberwachung beschrieben: Genannt werden Kommunikationsmittel im Allgemeinen. Wie im Fernmeldegesetz und im BÜPF werden bewusst nicht die technischen Mittel im Einzelnen genannt, um in diesem Gebiet, in dem die technische Entwicklung besonders rasant voranschreitet, die nötige Handlungsfreiheit zu bewahren. Materiell bedarf es konkreter Hinweise, die vermuten lassen, dass ein mutmasslicher Gefährder oder eine mutmassliche Gefährderin diese Mittel dazu benützen, um mit Personen Informationen auszutauschen oder Handlungen zu vollziehen, die einen direkten Bezug zur konkreten Gefährdung der inneren oder äusseren Sicherheit aufweisen. Damit zu einem gegebenen Zeitpunkt eine Überwachung gerechtfertigt ist, müssen diese Hinweise hinreichend konkret und aktuell sein. Allgemeine Erkenntnisse aus der Vergangenheit über mögliche Gefährdungen genügen nicht.

Abs. 2

Die Bestimmung betreffend die Überwachung einer öffentlichen Fernmeldestelle entspricht der Sonderregelung von Artikel 4 Absatz 2 BÜPF. In der Praxis handelt es sich um Fälle, in denen beispielsweise aus der Observation einer Zielperson oder aus anderen Fernmeldeüberwachungen bekannt ist, dass eine Zielperson regelmässig oder für bestimmte Kontakte eine bestimmte öffentliche Telefonzelle benutzt.

Abs. 3

Wenn eine Zielperson den Fernmeldeanschlusses in rascher Folge wechselt, zum Beispiel durch den Einsatz von Prepaid-Karten in der Mobiltelefonie, käme eine Anordnung im Einzelfall fast immer zu spät. In diesen Fällen kann eine Anordnung getroffen werden, dass alle identifizierten Anschlüsse, welche die Person oder Organisation benutzt, überwacht werden können. Auch diese Bestimmung hat ihr Vorbild im BÜPF (Art. 4 Abs. 4).

Abs. 4

Für die Durchführung der präventiven Post- und Fernmeldeüberwachungen sollen keine Parallelstrukturen zum BÜPF geschaffen werden. Deshalb gelten für die Formen der Überwachung, ihre technische Umsetzung und die Entschädigungen das BÜPF und dessen Ausführungserlasse sinngemäss.

Öffentliches Interesse und Verhältnismässigkeit

Die Überwachung des Post- und Fernmeldeverkehrs ist eine schwerwiegende Einschränkung der Privatsphäre. Nach Artikel 36 BV müssen Einschränkungen von Grundrechten durch ein öffentliches Interesse gerechtfertigt sein und im Vergleich zum angestrebten Zweck verhältnismässig sein. In Bezug auf das öffentliche Interesse darf das Mittel der Überwachung des Post- und Fernmeldeverkehr – wie alle anderen besonderen Mittel der Informationsbeschaffung – nur in den drei Bereichen eingesetzt werden, aus denen eine Gefährdung entstehen kann, die an die Grundstrukturen unserer Gesellschaft rührt (vgl. Kommentar zu Art. 13*a* Abs. 1). Entsprechend ist das öffentliche Interesse an dieser Massnahme evident. Für die Beurteilung der Verhältnismässigkeit der Massnahme gilt es zu prüfen, ob sie angemessen und notwendig ist und ob sie in einem vernünftigen Verhältnis zum angestrebten Zweck steht. Liegen hinreichende Anhaltspunkte vor, dass der mutmassliche Gefährder oder die mutmassliche Gefährderin für seine Umtriebe Fernmeldemittel benutzt, stellt diese Form der Überwachung das angemessene Mittel dar, um

Informationen zu gewinnen, anhand derer die Gefährdung besser beurteilt und ihr vorgebeugt werden kann.

Die Sicherheitsorgane sind indessen nicht berechtigt, Überwachungen im Sinne einer reinen Sondierung durchzuführen, nur weil eine Annahme besteht, dass eine Person eine Gefahr für die innere Sicherheit darstellen könnte. Vielmehr bedarf es in jedem Fall konkreter Anhaltspunkte für die Gefährdung und den Umstand, dass sich die jeweilige Person für ihre Umtriebe bestimmter Fernmeldemittel bedient.

In Bezug auf die Notwendigkeit der Massnahme ist offensichtlich, dass sich das Kontaktnetz einer Person, von der eine Gefahr ausgeht, oder der Inhalt der über Fernmeldemittel ausgetauschten Mitteilungen, einzig mittels Fernmeldeüberwachung hinreichend in Erfahrung bringen lassen. Allein mit der allgemeinen Informationsbeschaffung nach Artikel 14 Absatz 2 lassen sich solche Informationen kaum beschaffen.

Ob die Massnahme im engen Sinn des Wortes verhältnismässig ist – d.h. ob das öffentliche Interesse in dem Masse überwiegt, das der Eingriff in die Grundrechte der Person gerechtfertigt ist – lässt sich nicht allgemein-abstrakt festlegen. Durch die enge Aufgabenumschreibung des BWIS ist der Einsatzbereich bereits gesetzlich stark eingeschränkt. Eine weitere Einschränkung im Sinne eines Deliktskatalogs wie im Strafprozessrecht wäre sachfremd, weil gerade keine Vermischung mit strafrechtlich relevanten Verdachtslagen erfolgen darf und weil sich die Präventionstätigkeit ihrer Funktion entsprechend nicht an klaren Straftatbeständen orientieren kann. Nur in Kenntnis der fallspezifischen Umstände können die verantwortlichen Organe zwischen öffentlichem Interesse und der Wahrung der Grundrechte des oder der Einzelnen abwägen und einen fundierten Entscheid zu fällen. Wichtig ist, dass nicht allein die Sicherheitsorgane, sondern eine unabhängige richterliche Instanz die rechtlichen Aspekte beurteilt. Sie ist am besten in der Lage, die Bedürfnisse der Sicherheitsorgane und den legitimen Anspruch aller, ohne staatliche Einmischung mit anderen zu kommunizieren und Kontakte zu pflegen, unabhängig und nach gesetzlichen Kriterien gegeneinander abzuwägen.

Im Rahmen dieser Erwägungen und in Berücksichtigung der im Gesetzesentwurf vorgesehenen Einschränkungen und Vorkehrungen, ist die präventive Überwachung des Post- und Fernmeldeverkehrs ein zur Wahrung des öffentlichen Interesses verhältnismässiges Mittel. Es kann in Übereinstimmung mit den Anforderungen der Verfassung und der Menschenrechtskonventionen eingesetzt werden.

Art. 18l Beobachten an nicht allgemein zugänglichen Orten, auch mittels technischem Überwachungsgerät

Nach den geltenden Bestimmungen des BWIS dürfen die Sicherheitsorgane an öffentlichen und allgemein zugänglichen Orten Vorgänge beobachten und diese auch mit Bild- und Tonaufzeichnungen festhalten (Art. 14 Abs. 2 Bst. f BWIS). Mit der neuen Bestimmung soll es nun möglich werden, auch an nicht allgemein zugänglichen Orten zu beobachten und aufzuzeichnen (beispielsweise in gewerbsmässig genutzten Räumen, Versammlungslokalen, Wohnungen, Hotelzimmern; vgl. Abs. 1). Dazu ist neu auch der Einsatz technischer Überwachungsgeräte vorgesehen (vgl. Abs. 2). Nach geltendem Recht ist es verboten, solche Mittel einzusetzen, um nichtöffentliche Gespräche abzuhören oder aufzuzeichnen (vgl. Art. 179bis und 179ter StGB). Verboten ist auch, einen Vorgang aus dem Geheim- oder Privatbereich einer Person mit einem Aufnahmegerät zu beobachten oder aufzuzeichnen (Art. 179^{quater} StGB), wenn sich ein

solcher Vorgang zwar an einem allgemein zugänglichen Ort abspielt, aber von den Beteiligten willentlich der Öffentlichkeit entzogen wird. Nicht geschützt dagegen ist allgemeines privates Verhalten in der Öffentlichkeit.

Abs. 1

Diese Bestimmung legt die Einzelheiten der Beobachtung fest und umschreibt die Bedingungen, unter denen sie durchgeführt werden darf. Es müssen konkrete und aktuelle Tatsachen vorliegen, die vermuten lassen, dass die betreffende Person einen bestimmten Ort nutzt, um mit anderen zu kommunizieren oder um Handlungen zu vollziehen, die einen direkten Bezug zu der konkreten Gefährdung der inneren oder äusseren Sicherheit aufweist.

Abs. 2

Der Einsatz technischer Überwachungsgeräte entspricht in Regelung und Umfang der Bestimmung von Artikel 66 Absatz 2 des Bundesgesetzes vom 15. Juni 1934[50] über die Bundesstrafrechtspflege. Es handelt sich um akustische und optische Beobachtungs- und Aufzeichnungsgeräte. Diese Geräte können bei Vorliegen der entsprechenden Voraussetzungen auch in einem privaten Umfeld eingesetzt werden. Ebenfalls unter diese Bestimmung fällt das technische Beobachten und Aufzeichnen von Vorgängen, die privater Natur sind, obwohl sie sich an einem allgemein zugänglichen Ort abspielen, wie etwa ein privates Gespräch in einem Restaurant.

Öffentliches Interesse und Verhältnismässigkeit

Das Beobachten an einem nicht allgemein zugänglichen Ort oder mithilfe technischer Überwachungsgeräte stellt einen schwerwiegenden Eingriff in die Privatsphäre dar. Wie bereits erwähnt, muss nach Artikel 36 BV ein solcher Eingriff durch ein öffentliches Interesse gerechtfertigt sein und im Verhältnis zum angestrebten Zweck stehen. Hinsichtlich der Rechtfertigung dieses besonderen Mittels durch ein öffentliches Interesse sei auf die Erläuterungen zu den Artikeln 13*a* und 18*k* verwiesen.

Zur Frage der Verhältnismässigkeit lassen sich die folgenden Überlegungen anstellen: Lässt sich aufgrund hinreichender Tatsachen feststellen, dass der mutmassliche Gefährder oder die mutmassliche Gefährderin für seine oder ihre Umtriebe einen bestimmten Ort nutzt, stellt die Beobachtung das angemessene Mittel dar, um nützliche Informationen zu gewinnen, anhand derer die Gefährdung beurteilt und ihr vorgebeugt werden kann. Die Sicherheitsorgane sind indessen nicht berechtigt, das gesamte private Umfeld einer Person zu beobachten, nur weil Grund zur Annahme besteht, dass sie eine Gefahr für die innere Sicherheit darstellen könnte. Die Beobachtung muss auf ein bestimmtes, konkretes Ziel ausgerichtet sein, das zentraler strategischer Bestandteil der Handlungen des mutmasslichen Gefährders oder der mutmasslichen Gefährderin ist. Lässt sich zwischen den als Gefahr erachteten Handlungen und der Nutzung eines Ortes ein Bezug hinreichend glaubhaft belegen, kann die Massnahme als angemessen bezeichnet werden.

Bezüglich der Notwendigkeit ist offensichtlich, dass sich abgesehen vom allfälligen Einsatz eines Informanten oder einer Informantin, die legalen Zugang zu den entsprechenden Orten haben, mit der allgemeinen Informationsbeschaffung nach Artikel 14 Absatz 2 BWIS keine Informationen über Vorgänge beschaffen lassen, die

[50] SR **312.0**

sich in Privaträumen abspielen. Nur ist es nicht immer möglich, in solchen Situationen Informanten oder Informantinnen zu gewinnen oder einzusetzen.

Die Verhältnismässigkeit im engeren Sinn, das heisst, das Abwägen, ob das öffentliche Interesse dasjenige der betroffenen Person überwiegt, lässt sich wie bereits gesagt, nur im konkreten Fall von den verantwortlichen Organen beurteilen. Die Entscheidung, ob in einem Fall ein rechtmässiges überwiegendes öffentliches Interesse besteht, ist dem Bundesverwaltungsgericht vorbehalten.

Der Einsatz technischer Überwachungsgeräte ist weniger ein eigenständiges Überwachungsmittel als vielmehr ein Hilfsmittel zur Beobachtung von Vorgängen, die sich in der Privatsphäre abspielen. Bei der mithilfe technischer Mittel durchgeführten Beobachtung treten diese Mittel lediglich an die Stelle einer beobachtenden Person, die in einem privaten Raum physisch gegenwärtig ist. Daraus folgt, dass aus denselben Gründen, aus denen das Beobachten von Vorgängen in einem privaten Raum als verhältnismässig bezeichnet werden kann, die mit technischen Geräten durchgeführte Beobachtung a priori als Mittel erachtet werden kann, das demselben Grundsatz der Verhältnismässigkeit entspricht. Ob ein überwiegendes öffentliches Interesse vorliegt, wird je nach Sachlage zu entscheiden sein.

Art. 18m Geheimes Durchsuchen eines Datenverarbeitungssystems

Die Nutzung von moderner EDV-Infrastruktur nimmt in der heutigen Gesellschaft eine immer wichtigere Rolle ein. Gerade das Internet ist zu einer wichtigen Plattform für den Austausch von Informationen geworden. Weil das öffentliche Internet von Sicherheitsbehörden heute bereits intensiv zur Informationsbeschaffung konsultiert wird, verlagern relevante Gruppen (etwa Terrororganisationen) die Verbreitung von heiklen Inhalten zunehmend in geschützte Bereiche, zu denen der Zugang beispielsweise mit Passwörtern gesichert ist. Ein Eindringen ist hier mit entsprechendem Fachwissen zwar möglich, jedoch strafrechtlich verboten (Art. 143bis StGB, unbefugtes Eindringen in ein Datenverarbeitungssystem).

Artikel 18*m* beschreibt, worum es sich bei diesem Mittel der besonderen Informationsbeschaffung handelt und wie es eingesetzt werden kann. Der Geltungsbereich erstreckt sich in Anlehnung an die entsprechenden Bestimmungen des Strafgesetzbuches (vgl. Art. 143 und 143bis StGB) auf elektronisch oder in vergleichbarer Weise gespeicherte Daten, die besonders gegen Zugriff Fremder gesichert sind. Im Gegensatz der im Rahmen einer Strafuntersuchung durchgeführten Durchsuchung, wird hier die Durchsuchung ohne das Wissen des mutmasslichen Gefährders durchgeführt. Es müssen wiederum hinreichend klare und aktuelle Tatsachen vorliegen, die vermuten lassen, dass die betreffende Person ein bestimmtes Datenverarbeitungssystem für ihre Umtriebe nutzt. Die Durchsuchung hat aber passiven Charakter. Das heisst, sie erlaubt nicht, so in das System einzugreifen, dass es funktionsuntüchtig wird oder seine Funktionen gestört oder Daten vernichtet werden. Zu denken ist etwa an die Suche nach Kontaktadressen im Laptop eines mutmasslichen Gefährders oder einer mutmasslichen Gefährderin oder an den Klartext einer chiffriert übermittelten E-Mail, die in einer bewilligten Fernmeldeüberwachung zwar festgestellt, aber nicht sichtbar gemacht werden konnte.

Als konkreter Anwendungsbereich drängt sich die Bearbeitung dschihadistischer Propaganda auf. Auch wenn sich diese nicht ausdrücklich gegen die Schweiz richtet, beinhaltet sie ein hohes Gefährdungspotenzial und ist entsprechend sicherheitsrelevant. In der jüngeren Vergangenheit wurde eine zunehmende Radikalisierung durch

dschihadistische Propagandaseiten und virtuelle Kontakte im Internet festgestellt. Zwar kann der DAP allgemein zugängliche Websites einsehen und sich an nicht geschützten Chaträumen beteiligen, doch hat er nach heutigem Recht keine Möglichkeit zum Eindringen in passwort- oder sonstwie gesicherte Bereiche, wo sich die entscheidenden Kontakte ereignen (z.B. im privaten Bereich von öffentlichen Chaträumen). Damit bleibt er von den massgebenden Bereichen ausgesperrt, was im Interesse der Sicherheit der Schweiz geändert werden muss.

Öffentliches Interesse und Verhältnismässigkeit

Das Durchsuchen eines Datenverarbeitungssystems stellt eine schwerwiegende Einschränkung der Privatsphäre dar. Wie erwähnt muss gemäss Artikel 36 BV eine solche Einschränkung durch ein öffentliches Interesse gerechtfertigt sein und im Verhältnis zum angestrebten Zweck stehen. Hinsichtlich der Rechtfertigung dieses Mittels der Besonderen Informationsbeschaffung durch ein öffentliches Interesse sei auf die Erläuterungen zu den Artikeln 13*a* und 18*l* verwiesen. Bezüglich der Verhältnismässigkeit gilt Folgendes: Lässt sich mit einiger Wahrscheinlichkeit erkennen, dass der mutmassliche Gefährder oder die mutmassliche Gefährderin ein System und Datennetze nutzt, um für sich oder Dritte Daten zu bearbeiten oder zu speichern, die die innere oder äussere Sicherheit konkret gefährden, ist die Durchsuchung eines solchen Systems ein angemessenes und notwendiges Mittel, um die zur Beurteilung der Gefährdung notwendigen Informationen zu beschaffen. Es gibt kein anderes Mittel als in das Datenverarbeitungssystem einzudringen, um auf solche Daten zuzugreifen. Es sollen nur Datenverarbeitungssysteme durchsucht werden können, nicht aber beispielsweise Räume oder Fahrzeuge. Für diese sollen zur Informationsbeschaffung andere Mittel zur Verfügung stehen (z.B. physische Beobachtung oder technische Überwachungsgeräte). Die Revision schränkt hier die Auswahl an vorgesehenen Mitteln ein, um schon auf dieser Ebene die Verhältnismässigkeit zu wahren. Die Verhältnismässigkeit im engeren Sinn des Wortes – d.h. das Abwägen, ob das öffentliche Interesse die privaten Interessen der betroffenen Person überwiegt – lässt sich nur im konkreten Einzelfall beurteilen. Der Entscheid, ob im konkreten Fall ein überwiegendes öffentliches Interesse besteht, ist dem Bundesverwaltungsgericht vorbehalten.

Kapitel 3*b*: Verbot von Tätigkeiten und Bekämpfung von Gewaltpropaganda

Als neue Massnahme wird das Verbot bestimmter Tätigkeiten eingeführt. Die vom Parlament am 24. März 2006 verabschiedete Revision des BWIS (Gewaltpropaganda, Gewalt bei Sportveranstaltungen) war ein erster Schritt in diese Richtung: Rayonverbot, Ausreisebeschränkung, Meldeauflage und Polizeigewahrsam sollen das Verhalten von Privatpersonen lenken und so Gewalttätigkeiten an Sportveranstaltungen verhindern. Die vorliegende Revision geht auch in diese Richtung: Die präventive Gefahrenabwehr soll lenkend auf das Verhalten von Privatpersonen einwirken können.

Art. 18n Verbot von Tätigkeiten

Mit dieser Bestimmung erhält der Vorsteher oder die Vorsteherin des EJPD die Kompetenz, gegen bestimmte Tätigkeiten gerichtete verwaltungsrechtliche Verbote

zu verhängen, soweit die fragliche Tätigkeit mit einer konkreten Gefährdung der inneren oder äusseren Sicherheit der Schweiz einhergeht.

Nach heutigem Recht können solche Verbote nur gestützt auf die BV und unter sehr hohen Voraussetzungen verhängt werden. Die BV ermächtigt den Bundesrat, Verordnungen und Verfügungen zur Wahrung der Landesinteressen zu erlassen (Art. 184 Abs. 3 BV) und Massnahmen gegen unmittelbar drohende schwere Störungen der öffentlichen Ordnung oder der inneren oder äusseren Sicherheit der Schweiz zu treffen (Art. 185 Abs. 3 BV). Alle auf diesen beiden verfassungsrechtlichen Bestimmungen gestützten Verordnungen müssen indessen befristet werden und können nicht auf unbegrenzte Zeit immer wieder verlängert werden. Andernfalls würde die Verfassung ausgehöhlt. Deshalb soll auf Gesetzesebene eine Möglichkeit geschaffen werden, bei gegebener Gefährdung der Sicherheit der Schweiz bestimmte Tätigkeiten verbieten zu können.

Die neue Bestimmung berührt die erwähnten Kompetenzen des Bundesrates nach den Artikeln 184 Absatz 3 und Artikel 185 Absatz 3 BV nicht. Sie bleiben parallel weiter bestehen (vgl. auch Erläuterung zu den Art. 18*e* in fine und 29*a* Abs. 1).

Der Rechtsmittelweg verläuft bei Verboten oder Massnahmen, die vom Bundesrat kraft der Bundesverfassung verhängt werden, anders als bei einem Verbot durch das Departement gemäss der vorgeschlagenen Neuregelung. Die Entscheide des Bundesrates sind Regierungsakte; sie können nur dann vor einem Bundesgericht angefochten werden, wenn das Völkerrecht einen Anspruch auf gerichtliche Beurteilung einräumt[51]. Ist dem nicht so, sind Entscheide des Bundesrates endgültig. Demgegenüber ist vorgesehen, dass gegen gestützt auf das BWIS ergangene Verfügungen die Beschwerde an das Bundesverwaltungsgericht möglich ist, dessen Entscheid an das Bundesgericht weiterziehbar ist.

Mit der vorgeschlagenen Neuregelung geht eine vom Völkerrecht losgelöste und weit reichende Stärkung des Rechtsschutzes einher (der Rechtsmittelweg führt via Bundesverwaltungsgericht an das Bundesgericht). Die in diesem Zusammenhang von vereinzelten Vernehmlassungsteilenehmerinnen und -teilnehmern erhobene Kritik, die Beschwerdemöglichkeit laufe auf eine Umkehr der Beweislast hinaus, findet weder im Gesetzesentwurf eine Grundlage, noch wird solches angestrebt. Im Gegenteil: Korrelat der neuen Kompetenz soll und muss ein starker Rechtsschutz sein!

Soweit im Vernehmlassungsverfahren im Zusammenhang mit vorliegendem Artikel die Schaffung einer Rechtsgrundlage zur Beschlagnahme von Insignien radikaler Organisationen anbegehrt wurde, wird auf die gesonderten Gesetzgebungsarbeiten zum Bundesgesetz über Massnahmen gegen Rassismus verwiesen.

Abs. 1

Mit dieser Bestimmung sollen bestimmte Tätigkeiten verboten werden können. So gibt es Handlungsweisen, die auf den ersten Blick harmlos oder gar fördernswert scheinen, wie beispielsweise Geldsammlungen für einen in einem ausländischen Krisengebiet gelegenen Witwen- und Waisenfonds. Nicht selten gelangen dabei aber einerseits erpressungsähnliche Druckmassnahmen zur Anwendung (zum Beispiel

51 Vgl. BGE **125** II 417 ff.; Diese Rechtsprechung ist auch in Art. 83 Bst. a des Bundesgerichtsgesetzes vom 17. Juni 2005 (SR **173.110**) und in Art. 32 Abs. 1 Bst. a des Verwaltungsgerichtsgesetzes (SR **173.32)** verankert.

werden die Mitglieder der hier ansässigen Diaspora direkt auf im Heimatland verbliebene Familienangehörige angesprochen und diesen für den Fall einer verweigerten Spende Benachteiligungen in Aussicht gestellt). Anderseits werden die so gesammelten Gelder aller Wahrscheinlichkeit nach nicht dem in der Schweiz für die Sammlung vorgeschobenen, sondern mindestens teilweise einem ganz anderen Zweck zugeführt, wie beispielsweise dem Kauf von Waffen für eine im Krisengebiet aktive Widerstandsbewegung. Für solche Machenschaften lässt sich indessen oft kaum direkter Beweis erbringen: Die in der Schweiz zu Spenden genötigten Personen schweigen aus Angst um sich und ihre im Heimatland verbliebenen Familienangehörigen, Freunde und Bekannte. Der Transfer des Geldes ins Ausland lässt sich zwar verfolgen, doch verliert sich dann die Spur des Geldes in verschlungenen Geldtransfers, in mangelnden, gefälschten oder korrupt erlangten echten, aber inhaltlich falschen ausländischen Bescheinigungen über die Verwendung des Geldes und so fort. Auch direkte Nachfragen im Zielland scheiden wegen der möglichen Gefährdung der involvierten Personen aus. Hinzu kommt, dass die zur Spendensammlung benutzten Organisationen oft häufig den Namen wechseln, ihr Auftreten immer wieder ändern und zur «Spendensammlung» nicht selten im Ausland wohnhafte Drittpersonen einsetzen.

Der Departementsvorsteher oder die Departementsvorsteherin muss Umfang und Inhalt des Verbotes so genau wie möglich umschreiben. Geprüft und verworfen wurde die im Vernehmlassungsverfahren teilweise geforderte Auflistung von verbotenen Handlungen im Gesetz: Eine solche Liste mit verbotenen Handlungen wäre einerseits eine direkte Einladung zur Umgehung, und andererseits bestünde keine Möglichkeit, andere oder neue Bedrohungsformen rasch zu unterbinden. Sollen möglichst alle Schattierungen des unerwünschten Verhaltens erfasst werden, lassen sich die Kriterien kaum enger fassen.

Entgegen der Befürchtung einzelner Vernehmlassungsteilnehmerinnen und -teilnehmer ist das Tätigkeitsverbot kein Instrument zur Bekämpfung der Opposition. Vielmehr richtet es sich gegen alle, die einerseits terroristische oder gewaltextremistische Umtriebe fördern und kumulativ andererseits dadurch die innere oder äussere Sicherheit der Schweiz konkret gefährden. Mit diesem verwaltungsrechtlichen Verbot soll also nicht in erster Linie eine Straftat, sondern eine Gefährdung der inneren Sicherheit (die nicht a priori strafbar sein muss) vermieden werden.

In der Verbotsverfügung muss auf die Strafdrohung nach Artikel 292 StGB hingewiesen werden, soweit bei Ungehorsam eine Bestrafung erfolgen soll. Ein gesetzlicher Verweis auf die strafrechtliche Norm erübrigt sich, da ihm bloss deklaratorischer Charakter zukäme.

Abs. 2

Verbote nach Absatz 1 können die Betroffenen an der Ausübung von Grundrechten hindern. Es ist deshalb wichtig, solche Verbote zu befristen. So werden die Behörden gezwungen, nach Ablauf der Gültigkeit eines Verbotes wiederum zu prüfen, ob die Anordnungsvoraussetzungen nach wie vor erfüllt oder ob sie dahingefallen sind.

Sind die Anordnungsvoraussetzungen nach wie vor erfüllt, kann die Gültigkeitsdauer eines Verbots so lange verlängert werden, wie es die Umstände erfordern. Als Folge der jeweiligen Befristung wird das Departement ausdrücklich verpflichtet, regelmässig zu prüfen, ob die Anordnungsvoraussetzungen noch erfüllt sind, und allenfalls das Verbot umgehend aufzuheben. Das Departement ist also gehalten,

nicht nur aktiv zu werden, um ein Verbot zu verhängen, sondern ebenso, wenn es darum geht, ein einmal verhängtes Verbot wieder aufzuheben.

Öffentliches Interesse und Verhältnismässigkeit

Das Verbot von Tätigkeiten ist ein schwerer Grundrechtseingriff und kann mehrere Grundrechte tangieren, soweit diese Grundrechte die entsprechenden Tätigkeiten schützen, so beispielsweise die Vereinigungsfreiheit (Art. 23 BV), die Glaubens- und Gewissensfreiheit (Art. 15 BV), die Meinungs- und Informationsfreiheit (Art. 16 BV), die Versammlungsfreiheit (Art. 22 BV) oder die Eigentumsgarantie (Art. 26 BV). Nach Artikel 36 BV müssen solche Beschränkungen vor allem durch ein öffentliches Interesse gerechtfertigt und verhältnismässig sein. Das öffentliche Interesse ergibt sich ohne Weiteres aus der im Aufgabenbereich des BWIS verankerten Pflicht, frühzeitig Gefährdungen durch Terrorismus und gewalttätigen Extremismus zu erkennen und zu bekämpfen. In Bezug auf die Verhältnismässigkeit ist festzuhalten, dass das Verbot einer bestimmten Tätigkeit unter den im Gesetz genannten Bedingungen nicht a priori unverhältnismässig ist. Vielmehr ist die erforderliche Güterabwägung im konkreten Einzelfall vorzunehmen.

Art. 18o Sicherstellung, Beschlagnahme und Einziehung von Propagandamaterial

Der durch Ziffer I des BG vom 24. März 2006 (in Kraft seit 1. Jan. 2007) eingefügte Artikel 13*a* muss wegen der notwendigen Neugliederung des BWIS innerhalb des Gesetzes verschoben werden. Er wird neu als Artikel 18*o* aufgeführt. Der Wortlaut ist mit der bisherigen Fassung identisch; materielle Änderung erfolgt keine.

Art. 27 Abs. 1bis

Artikel 27 des Gesetzes verpflichtet den Bundesrat, die eidgenössischen Räte, die Kantone und die Öffentlichkeit jährlich oder nach Bedarf über seine Beurteilung der Bedrohungslage und über die Tätigkeiten der Sicherheitsorgane des Bundes zu orientieren. Daran anknüpfend soll das Departement verpflichtet werden, jährlich oder nach Bedarf über die Verwendung der mit vorliegender Revision neu eingeführten Mittel zu informieren (z.B. im Rahmen des Berichts «Innere Sicherheit der Schweiz»). Angesichts der möglichen Beschränkung von Grundrechten der Bevölkerung versteht sich eine solche Berichterstattung von selbst. Es betrifft dies den Einsatz von Tarnidentitäten, der besonderen Mittel der Informationsbeschaffung sowie das Verbot von Tätigkeiten. Im Übrigen erfolgt bereits heute und ohne ausdrückliche gesetzliche Anordnung eine umfassende Berichterstattung an das Departement und die Geschäftsprüfungsdelegation.

Kapitel 6*a*: Verfahren und Rechtsschutz

Art. 29a

Mit der Einführung der besonderen Mittel der Informationsbeschaffung entsteht beim Rechtsschutz Anpassungsbedarf an die Erfordernisse der BV und der EMRK. Von besonderer Bedeutung sind dabei die Artikel 29*a* BV (Rechtsweggarantie) und Artikel 13 EMRK (Recht auf eine wirksame Beschwerde).

Im Vernehmlassungsverfahren wurde die im damaligen Absatz 2 der Bestimmung ursprünglich vorgesehene Beschränkung der Kognition auf die Verletzung von Bundesrecht stark kritisiert. Diese Kritik wurde aufgenommen und die Kognition für das Beschwerdeverfahren auf die unrichtige oder unvollständige Feststellung des rechtserheblichen Sachverhaltes erweitert (vgl. Erläuterung zu Abs. 3). Damit wurde ein wirksamer Rechtsschutz als Korrelat zu erweiterten nachrichtendienstlichen Befugnissen geschaffen.

Abs. 1

Diese Bestimmung verankert das Beschwerderecht gegen gestützt auf das BWIS ergangene Verfügungen von Bundesorganen. Damit wird auch Artikel 32 Absatz 1 Buchstabe a des Verwaltungsgerichtsgesetzes präzisiert, indem klar festgelegt wird, dass die erwähnten Entscheide gemäss BWIS justiziable Verwaltungsverfügungen sind und nicht zur Kategorie der Regierungsakte gehören. Regierungsakte sind im Regelfall gerade nicht beim Bundesverwaltungsgericht anfechtbar (vgl. auch Erläuterung zu Art. 18*n*).

Abs. 3

Die Beschwerdeführerin oder der Beschwerdeführer kann mit der Beschwerde die Verletzung von Bundesrecht einschliesslich Überschreitung oder Missbrauch des Ermessens sowie die unrichtige oder unvollständige Feststellung des rechtserheblichen Sachverhaltes rügen.

Anhang: Änderung bisherigen Rechts

1. Verwaltungsgerichtsgesetz vom 17. Juni 2005[52]

Die Einführung von Artikel 13*b* BWIS bedingt die Ergänzung von Artikel 35 Bst. d des Verwaltungsgerichtsgesetzes. Artikel 13*b* BWIS legt nämlich fest, dass das Bundesverwaltungsgericht zuständig ist, Streitigkeiten zu schlichten zwischen dem Bundesamt für Polizei und den Behörden, kantonalen Verwaltungseinheiten, den Organisationen, die öffentliche Aufgaben erfüllen, wie auch den Bundesorganen, die nicht der zentralen Bundesverwaltung angehören (vgl. auch Erläuterung zu Art. 13*b*).

2. Schweizerisches Strafgesetzbuch[53]

Art. 179^{octies}

Der Einsatz von technischen Überwachungsgeräten, wie Ton- und Bildaufzeichnungsgeräten im Geheimbereich, sind strafbare Handlungen im Sinne der Artikels 179ff StGB. Der Artikel 179^{octies} behält indessen die amtliche Überwachung nach Massgabe des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vor.

52 SR **173.32**
53 SR **311.0**

Diese Strafbestimmung muss deshalb angepasst werden, damit auch die neuen, im Verfahren nach BWIS durchgeführten Überwachungsmassnahmen vorbehalten bleiben.

Art. 317bis

Urkundenfälschung ist eine strafbare Handlung (vgl. Art. 251, 252, 255, 317, StGB). Der heutige Artikel 317bis StGB behält indessen die Herstellung und Verwendung gefälschter Urkunden vor, die zum Aufbau oder zur Aufrechterhaltung einer Legende im Rahmen einer richterlich genehmigten verdeckten Ermittlung verwendet werden. Diese Strafbestimmung muss angepasst werden, damit auch die Verwendung der Tarnidentitäten gemäss BWIS vorbehalten bleiben.

3. Bundesgesetz über die Armee und die Militärverwaltung[54]

Art. 99 Abs. 1, zweiter Satz, Abs. 1bis und 2

Abs. 1 zweiter Satz

Die in Artikel 99 Absatz 1 des Gesetzesentwurfs vorgesehene (grundsätzliche) Beschränkung der Funkaufklärung auf Ziele im Ausland soll die Empfehlung 1 der Geschäftsprüfungsdelegation aus deren Bericht vom 10. November 2003 zum Projekt ONYX umsetzen. Unter Funkaufklärung gegen Ziele im Ausland ist die Erfassung von elektromagnetischen Ausstrahlungen im Ausland zu verstehen. Heute geschieht dies mittels des Systems ONYX für den Bereich der Satellitenkommunikation oder mittels Kurzwellenempfangsanlagen für dieses Frequenzspektrum. Welche Mittel und Systeme in Zukunft für einen auf das Ausland bezogenen Funkaufklärungsauftrag eingesetzt werden, wird eine Frage der technischen Entwicklung sein. Der Gesetzestext lässt dies mit der allgemeinen Formulierung «Funkaufklärung» bewusst offen.

Abs. 1bis

Die Funkaufklärung soll nach Absatz 1 zweiter Satz grundsätzlich gegen Ziele im Ausland eingesetzt werden. Es gibt jedoch weiterhin Funkaufklärungsbedürfnisse der Armee im Inland. Angesichts des grundsätzlichen Charakters der Regel von Absatz 1 zweiter Satz und des Umstandes, dass Einschränkungen der Grundrechte wie desjenigen auf der Wahrung der Privatsphäre einer formellgesetzlichen Grundlage bedürfen, muss der Einsatz der Funkaufklärung im Inland gegen Zivilpersonen explizit geregelt werden. Absatz 1bis sieht deshalb die folgenden beiden Fälle vor, bei denen die Funkaufklärung der Armee im Inland gegen Zivilpersonen gestattet ist:

Buchstabe a bezieht sich auf die Überwachung der militärisch genutzten Frequenzen im Inland. Die Armee soll zum einen bei ihren Einsätzen militärisch genutzte Frequenzen auf allfällige zivile Nutzer überprüfen können. Zum anderen soll sie, mit eigenen Mitteln, alle militärisch genutzten Frequenzen aufklären und überwachen können. Gegebenenfalls wird die Armee zivile Frequenznutzer identifizieren und ausfiltern. Nur so können die militärische Nutzung der Frequenzen sichergestellt und Missbräuche verhindert werden.

54 SR **510.10**

Buchstabe b bezieht sich auf die Wahrung der Lufthoheit. Die Luftwaffe hat nach der Verordnung vom 23. März 2005[55] über die Wahrung der Lufthoheit (VWL) die Lufthoheit sicherzustellen. Sie muss zu diesem Zweck mittels Funkaufklärung den Funkverkehr zwischen militärischen und zivilen Flugzeugen und ihren (zivilen oder militärischen) Bodenstationen erfassen können. Auf diese Weise können u.a. unbekannte Flugobjekte erkannt, identifiziert und gegebenenfalls die richtigen Abwehrmittel ergriffen werden. Die Funkaufklärung dient der Luftwaffe auch zur generellen Überwachung des Luftraums und zur Darstellung der Luftlage, wozu sie nach Artikel 5 VWL verpflichtet ist.

Des Weiteren ist der Einsatz der Funkaufklärung durch die Armee gegen zivile Ziele im Inland (oder im Ausland) auch dann gestattet, wenn er im Rahmen der Notwehr oder des Notstandes erfolgt, zum Beispiel um Armeeangehörige vor einem bevorstehenden Angriff durch Zivilpersonen zu schützen. Es handelt sich hier um einen klassischen Rechtfertigungsgrund, der im Militärgesetz nicht explizit vorgesehen werden muss, da er in den Artikeln 25 und 26 des Militärstrafgesetzes vom 13. Juni 1927[56] (MStG) bereits hinlänglich geregelt ist.

Art. 99 Abs. 2

Absatz 2 in seinem jetzigen Wortlaut ermächtigt den strategischen Nachrichtendienst, Personendaten zu bearbeiten. Vor allem hinsichtlich der Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen entspricht diese Bestimmung aber nicht vollauf den allgemeinen Grundlagen des Datenschutzes. Um diesen Standards zu genügen, soll Artikel 99 Absatz 2 so ergänzt werden, dass die in den Absätzen 1 und 2 des aktuellen Artikels 15 BWIS genannten Datenbearbeitungsprinzipien im Wesentlichen übernommen werden.

Der zweite und dritte Satz von Absatz 2 sind inhaltlich aus Artikel 15 Absatz 1 BWIS übernommen worden. Sie betreffen die Bearbeitung aller Personendaten und verankern die allgemeinen Grundsätze hinsichtlich der Beurteilung der Richtigkeit von Daten und der Vernichtung unrichtiger oder nicht notwendiger Daten (vgl. Art. 4 und 5 DSG).

Darüber hinaus wurde die heutige Regelung gemäss Artikel 9 Absatz 1 Buchstaben a–c der Nachrichtendienstverordnung VBS vom 26. September 2003[57] (VND) übernommen, womit die Voraussetzungen für die Bearbeitung besonders schützenswerter Personendaten und von Persönlichkeitsprofilen neu direkt im MG geregelt werden. Die weitergehende Konkretisierung erfolgt durch den Bundesrat auf Verordnungsstufe.

Mit der vorgeschlagenen Anpassung von Artikel 99 Absatz 2 MG wird dahin gewirkt, dass die beiden Dienste SND und DAP Personendaten nach denselben Grundsätzen bearbeiten.

Art. 99a

In Übereinstimmung mit Artikel 164 Absatz 1 BV müssen alle wichtigen rechtsetzenden Normen in Form eines formellen Gesetzes erlassen werden. Die heutigen

55 SR **748.111.1**
56 SR **321**
57 SR **510.291**

Bestimmungen zur Funkaufklärung in der Verordnung über die elektronische Kriegsführung enthalten rechtsetzende Normen, haben aber keine ausdrückliche formellgesetzliche Grundlage im Militärgesetz. Es gilt deshalb, für diese Bestimmungen eine angemessene Rechtsgrundlage zu schaffen.

Abs. 1

Mit dieser Bestimmung wird die heutige «Unabhängige Kontrollinstanz» (UKI) auf Gesetzesebene verankert. Derzeit dienen die Bestimmungen in Artikel 14 ff. der Verordnung vom 15. Oktober 2003[58] über die elektronische Kriegsführung als Rechtsgrundlage dieser Instanz.

Die unabhängige Kontrollinstanz kontrolliert grundsätzlich nur Funkaufklärungsaufträge, für die keine besondere (Einzel-) Bewilligung auf politischer Stufe vorgesehen ist, wie dies bei den Aufträgen (z.B. des strategischen Nachrichtendienstes des VBS) für die ständige Funkaufklärung der Fall ist. Funkaufklärung im Ausland (durch die Armee) kann aber auch im Rahmen eines Friedensförderungsdienstes stattfinden. Hier schliesst der entsprechende Parlamentsbeschluss die Bewilligung für die Funkaufklärung mit ein. Weil in diesen Fällen eine Bewilligung der zuständigen politischen Behörde vorliegt, erfolgt keine zusätzliche Überprüfung des Funkaufklärungsauftrages durch die unabhängige Aufsichtsbehörde.

Die Instanz kontrolliert die Rechtmässigkeit der ständigen Funkaufklärung, was auch die Kontrolle der Verhältnismässigkeit der Massnahme impliziert. Die Instanz spricht sich indessen nicht zur Zweckmässigkeit der Kontrolle aus.

Damit ihre Unabhängigkeit gewährt ist, verrichtet die Instanz ihre Aufgaben weisungsunabhängig.

4. Fernmeldegesetz vom 30. April 1997[59]

Art. 44

Artikel 44 muss ergänzt werden, da neu für die Überwachung des Fernmeldeverkehrs nicht mehr nur das BÜPF gilt, sondern auch das BWIS. Die auf das BÜPF gestützte Überwachung des Post- und Fernmeldeverkehrs erfolgt im Rahmen eines Strafverfahrens des Bundes oder eines Kantons oder zum Vollzug eines Rechtshilfeersuchens nach dem Rechtshilfegesetz vom 20. März 1981[60]. Eine Überwachung des Post- und Fernmeldeverkehrs gestützt auf das BWIS wird zum Zwecke der Erkennung von Gefährdungen durch Terrorismus, verbotenen politischen oder militärischen Nachrichtendienst und verbotenen Handel mit Waffen und radioaktiven Materialien und verbotener Technologie durchgeführt.

58 SR **510.292**
59 SR **784.10**
60 SR **351.1**

5.–11.: Sozialversicherungsgesetze:

Bundesgesetz vom 20. Dezember 1946[61] über die Alters- und Hinterlassenenversicherung (AHVG);

Bundesgesetz vom 19. Juni 1959[62] über die Invalidenversicherung (IVG);

Bundesgesetz vom 25. Juni 1982[63] über die berufliche Alters-, Hinterlassenen und Invalidenvorsorge (BVG);

Bundesgesetz vom 18. März 1994[64] über die Krankenversicherung (KVG);

Bundesgesetz vom 20. März 1981[65] über die Unfallversicherung (UVG);

Bundesgesetz vom 19. Juni 1992[66] über die Militärversicherung (MVG);

Bundesgesetz vom 25. Juni 1982[67] über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung (AVIG)

Der Gesetzgeber hat im Bereich der Sozialversicherungen die Datenweitergabe in den jeweiligen Gesetzen selber geregelt und damit eine in sich geschlossene, umfassende und abschliessende Ordnung geschaffen. Entsprechend bedarf die Aufhebung des Amtsgeheimnisses gegenüber den Sicherheitsorganen von Bund und Kantonen nach Artikel 13*a* des vorliegenden Entwurfs der speziellen Anpassung dieser Gesetze. Dabei erfolgt keine umfassende Aufhebung des Amtsgeheimnisses, sondern eine auf die Bedingungen von Artikel 13*a* beschränkte. Gesetzliche Berufsgeheimnisse (z.B. Arzt, Anwalt, Geistlicher usw.) fallen nicht darunter und bleiben gewahrt. Im Übrigen erfolgt die Aufhebung des Amtsgeheimnisses analog bereits bestehender Regelungen für Strafuntersuchungsbehörden, Sozialhilfebehörden, Betreibungsämtern, Steuerbehörden, usw.

Zu betonen ist, dass die Auskunftspflicht ihrerseits auf die Bereiche Terrorismus, verbotener politischer oder militärischer Nachrichtendienst und Proliferation beschränkt ist. Einzig in diesem eng begrenzten Gefahrenbereich erfolgt eine Aufhebung des Amtsgeheimnisses.

Mit der laufenden Revision zur Änderung des Zivilgesetzbuches (Erwachsenenschutz, Personenrecht und Kindesrecht; vgl. BBl *2006* 7001) sollen im Sozialversicherungsbereich teilweise dieselben Gesetzesbestimmungen wie in der vorliegenden Revision des BWIS eingefügt werden. Zur Abstimmung dieser parallel laufenden

61 SR **831.10**
62 SR **831.20**
63 SR **831.40**
64 SR **832.10**
65 SR **832.20**
66 SR **833.1**
67 SR **837.0**

Revisionsvorhaben wird das Departement zu gegebener Zeit und entsprechend dem jeweiligen Stand der Gesetzesrevisionen Lösungsvorschläge unterbreiten.

3 Auswirkungen

3.1 Auswirkungen auf den Bund

3.1.1 Finanzielle Auswirkungen

Die finanziellen Auswirkungen sind stark abhängig von Art und Ausgestaltung der einzelnen Massnahmen und vor allem von der (ereignisabhängigen) Notwendigkeit derer Nutzung. Diesbezüglich bestehen noch keine Erfahrungswerte, insbesondere was die (in weiten Bereichen entscheidende) richterliche und exekutive Bewilligungspraxis betrifft. Aus den gleichen Gründen lassen sich auch keine konkreten Angaben zu einem allfälligen Sparpotenzial machen (z.B. Ersatz von Observationen durch Fernmeldeüberwachungen). Schätzungen ergaben für den technischen Bereich (Geräte, Ausrüstung) einmalige Investitionskosten von ca. 1 Million Franken und jährlich wiederkehrende Kosten von ca. 100 000 Franken sowie jährlich wiederkehrende Personalkosten von ca. 6,5 Millionen Franken (Arbeitgeberbeiträge miteingeschlossen). Die Finanzierung erfolgt durch eine departementsinterne Kompensation.

3.1.2 Personelle Auswirkungen

Für die Umsetzung der Massnahmen soll weitestgehend auf die bestehenden eidgenössischen (Bundesverwaltungsgericht, DAP) und kantonalen Strukturen (kantonale Polizeibehörden) aufgebaut werden. Insgesamt ist mit rund 40 zusätzlichen Stellen zu rechnen. Diese werden durch departementsinterne Kompensation geschaffen.

Der Stellenmehrbedarf besteht in folgenden Bereichen:

- 35 Stellen beim DAP für die Informationsbeschaffung und -auswertung (Polizisten und Polizistinnen, Dolmetscher und Dolmetscherinnen, Techniker und Technikerinnen, Analytiker und Analytikerinnen) sowie für die Anpassung der Datenverarbeitung (Datenerfassung, Qualitätssicherung, Verkehr mit dem Ausland);
- weitere 5 Stellen für die Anpassung vollzugsnotwendiger, aber nachrichtendienstfremder Verwaltungsstellen (z.B. für Technik und Administration im DBA des UVEK, das Bundesverwaltungsgericht und die Direktion fedpol).

Die zusätzlichen Kompetenzen sollen demnach weiterhin mit einem vergleichsweise bescheidenen Ressourcenansatz umgesetzt werden.

In der Vernehmlassung wurde vereinzelt bezweifelt, ob die heutige Zusammenarbeit der involvierten Stellen den Anforderungen genügt, und gefordert, die Aufgaben, Abläufe und Strukturen der betroffenen Verwaltungsstellen seien zu überprüfen.

Diesbezüglich ist einerseits auf die Stellungnahme des Bundesrates vom 2. Dezember 2005 zur Motion Schlüer (05.3637: Zusammenfassung der Nachrichtendienste im VBS und im EJPD) zu verweisen: «… Das Bundesamt für Polizei (Fedpol) wurde per 2001 im Sinne der Forderungen der PUK EJPD reorganisiert, sodass die Funktionen des Inlandnachrichtendienstes und der gerichtlichen Polizei nach den

Prinzipien der Organisation nach Prozessabläufen getrennt und intern verschiedenen Hauptabteilungen zugewiesen wurden. Diese stehen unter der Leitung des Direktors Fedpol, welcher dem Vorsteher des EJPD unterstellt ist. Der Bundesrat hält diese Aufgabenteilung und Organisation innerhalb des EJPD für effizient und sinnvoll …».

Anderseits äussert sich Ziffer 3 des Berichts «Effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen»[68] eingehend zur Zusammenarbeit von Strafverfolgungsorganen und Inlandnachrichtendienst. In Würdigung der gesamten Umstände sieht der Bundesrat keinen unmittelbaren Bedarf für neue gesetzliche oder politische Massnahmen im strukturellen Bereich. Darauf zurückzukommen besteht kein Anlass, zumal der Bundesrat diesbezüglich auch bei seinen Entscheiden zur Politik für die Nachrichtendienste und ihre Zusammenarbeit vom 24. Januar 2007 keinen weiteren Handlungsbedarf sah.

3.1.3 Sonstige Auswirkungen

Es sind keine spezifischen sonstigen Auswirkungen erkennbar.

3.2 Auswirkungen auf Kantone und Gemeinden

Das Sicherheitsniveau in den Kantonen und Gemeinden steigt. Den erhöhten Auskunfts- und Meldepflichten der kantonalen und kommunalen Verwaltungsstellen nach den Artikeln 13 und 13*a* des vorliegenden Entwurfes stehen mittel- bis langfristig gewissen Entlastungen (erleichterte Abklärungen, teilweise Ablösung der personalaufwendigen und entsprechend teuren Observationen kantonaler Polizeikräfte durch die besonderen Mittel der Informationsbeschaffung usw.) gegenüber, welche sich zum heutigen Zeitpunkt nicht beziffern lassen. Abhängig von der Art und Ausgestaltung der neuen Massnahmen ist denkbar, dass in den Kantonen zusätzliches Arbeitsvolumen entsteht.

3.3 Auswirkungen auf die Volkswirtschaft

Nach den Richtlinien des Bundesrates vom 15. September 1999 für die Darstellung der volkswirtschaftlichen Auswirkungen von Vorlagen des Bundes (BBl *2000* 1038) ist eine Vorlage nach folgenden Punkten zu prüfen:

3.3.1 Notwendigkeit und Möglichkeit staatlichen Handelns

Die Umsetzung der Vorlage erhöht die Sicherheit der Schweiz und dient u.a. der Umsetzung politischer Vorstösse.

68 Vgl. Bericht zum Postulat SiK

3.3.2 Auswirkungen auf die einzelnen gesellschaftlichen Gruppen

Die vorgeschlagenen Normen führen zu einer Stärkung der inneren und äusseren Sicherheit und damit zu einer Verbesserung des Schutzes der Bevölkerung.

3.3.3 Auswirkungen auf die Gesamtwirtschaft

Es sind keine direkten Auswirkungen auf die Gesamtwirtschaft ersichtlich. Indirekt werden durch ein sicheres und gesellschaftlich stabiles Umfeld die wirtschaftlichen Rahmenbedingungen verbessert, was den Standort Schweiz stärkt.

3.3.4 Alternative Regelungen

Für die innere Sicherheit seines Gebietes ist in erster Linie der Kanton verantwortlich. Soweit der Bund nach Verfassung und Gesetz für die innere Sicherheit verantwortlich ist, leisten ihm die Kantone Amts- und Vollzugshilfe. Nach geltendem Recht ist der Bund insbesondere zuständig zur frühzeitigen Erkennung von Gefährdungen durch Terrorismus, verbotenen Nachrichtendienst, gewalttätigen Extremismus, verbotenen Handel mit Waffen und radioaktiven Materialien sowie verbotenem Technologietransfer (Nonproliferation). Er unterstützt die zuständigen Polizei- und Strafverfolgungsbehörden durch Mitteilung von Erkenntnissen über das organisierte Verbrechen. Der Bund legiferiert somit in seinem Kompetenzbereich; Raum für alternative Regelungen besteht nicht.

3.3.5 Zweckmässigkeit im Vollzug

Die Umsetzung der Vorlage erfolgt auf der Grundlage der bewährten bisherigen Strukturen der Sicherheitsbehörden. Am Gesamtkonzept der gemeinsamen Verantwortung von Bund und Kantonen für den Staatsschutz ändert sich nichts.

3.4 Andere Auswirkungen

3.4.1 Auswirkungen auf die Aussenpolitik

Das internationale Ansehen der Schweiz kann sich nachhaltig verbessern, insbesondere was ihren Willen zur wirkungsvollen Bekämpfung des internationalen Terrorismus betrifft. Auch können Aktivitäten gewaltextremistischer ausländischer Gruppen in der Schweiz früher erkannt und besser kontrolliert werden, welche Forderung seit langem vom Sicherheitsausschuss des Bundesrates (SiA) erhoben wird.

3.4.2 Auswirkungen auf die internationalen Beziehungen

Die Gesetzesrevision setzt formal keine direkten internationalen Verpflichtungen um. Die Angleichung der Standards führt hingegen voraussichtlich zu einer deutlichen Verbesserung der internationalen Zusammenarbeit.

4 Verhältnis zur Legislaturplanung

Die Vorlage ist in der Legislaturplanung 2003–2007 (BBl *2004* 1149) nicht angekündigt.

Sie ist jedoch Teil des Bundesratsziels 19 für das Jahr 2007: «Die internationale Zusammenarbeit, die Prävention und die internen Strukturen in den Bereichen Polizei und Justiz optimieren».

Die Dringlichkeit und Notwendigkeit der Vorlage ergibt sich einerseits aus der in den letzten Jahren sukzessive verschlechterten Sicherheits- und Gefahrenlage der Schweiz, die sich namentlich durch die Terroranschläge islamistischer Täter deutlich akzentuiert hat. Westeuropa ist nicht länger nur Ruhe- und Vorbereitungsraum; die Schweiz gehört mit zum allgemeinen Gefahrenraum. Das heutige Gesetz nimmt Sicherheitsrisiken in Kauf, die mit der veränderten Bedrohungslage nicht mehr vereinbar sind. Auch die Fähigkeit zur internationalen Solidarität (so vor allem in der UNO und mit europäischen Staaten) ist gefährdet.

5 Rechtliche Aspekte

5.1 Verfassungsmässigkeit

Das BWIS stützt sich auf die ungeschriebene Bundeskompetenz zur Wahrung der inneren und äusseren Sicherheit der Eidgenossenschaft und die Aufgaben des Bundes zur Wahrung der inneren Sicherheit (Art. 173 BV). In diesem Rahmen bewegt sich auch die vorliegende Gesetzesrevision. Sie überschreitet den in Artikel 2 Absatz 1 und 2 BWIS verankerten heutigen Aufgabenbereich nicht, sondern ist im Anwendungsbereich einzelner Massnahmen auf Terrorismus, verbotenen militärischen und politischen Nachrichtendienst und Handel mit Waffen und radioaktiven Materialien sowie verbotenen Technologietransfer beschränkt. Weder verbotener wirtschaftlicher Nachrichtendienst noch organisierte Kriminalität bilden Gegenstand der besonderen Massnahmen zur Informationsbeschaffung der vorliegenden Gesetzesrevision.

Die im Rahmen der vorliegenden Revision vorgeschlagenen Massnahmen können in Grundrechte eingreifen. Tangiert werden können insbesondere die Privatsphäre (Art. 13 BV), die Vereinigungsfreiheit (Art. 23 BV), die Glaubens- und Gewissensfreiheit (Art. 15 Abs. 3 BV), die Versammlungsfreiheit (Art. 22 BV) und die Eigentumsgarantie (Art. 26 BV).

Nach dem Wortlaut von Artikel 36 BV bedürfen Einschränkungen von Grundrechten einer gesetzlichen Grundlage, müssen durch ein öffentliches Interesse oder durch den Schutz der Grundrechte Dritter gerechtfertigt sein und den Grundsatz der Verhältnismässigkeit wahren. Zudem darf der Kern der Grundrechte nicht verletzt werden. Einschränkungen eines Grundrechtes sind zulässig, sofern konkrete Rechts-

güter Dritter oder der Allgemeinheit in schwerwiegender Weise gefährdet oder verletzt werden.

Die vorgeschlagenen Mittel und Massnahmen sollen in einem Gesetz im formellen Sinn, dem BWIS, verankert werden. Das öffentliche Interesse besteht im Schutz der inneren oder äusseren Sicherheit sowie in der frühzeitigen Erkennung von Gefährdung durch Terrorismus, verbotenen politischen und militärischen Nachrichtendienst, verbotenen Handel mit Waffen und radioaktiven Materialien und verbotenen Technologietransfer. Zweifelsohne ist ein legitimes öffentliches Interesse vorhanden. Die Prüfung der Verhältnismässigkeit der neuen Massnahmen ist in den Erläuterungen zu den einzelnen Gesetzesartikeln kommentiert. In diesem Zusammenhang ist auch in Erinnerung zu rufen, dass bei der Prüfung der Verhältnismässigkeit des staatlichen Eingriffs die mit den jeweiligen Massnahmen einhergehenden Begleitumstände im Einzelfall zu berücksichtigen sind (so auch die Stellungnahme des Bundesgerichts im Vernehmlassungsverfahren). Im Übrigen ergibt sich aus den Anordnungsvoraussetzungen für besondere Mittel der Informationsbeschaffung nach Artikel 18*b*, insbesondere Buchstaben c, unmissverständlich die subsidiäre Natur von Massnahmen mit Grundrechtseingriffen. Sie sollen mit anderen Worten nur zur Anwendung gelangen, wenn sich andere Informationsbeschaffungsmassnahmen für die Abklärung eines konkreten Verdachts einer Gefährdung der inneren oder äusseren Sicherheit der Schweiz als unzureichend erweisen.

Die einzelnen Mittel und Massnahmen der Vorlage sind verfassungskonform; die rechtsstaatlichen Prinzipien werden vollumfänglich gewahrt.

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Als Vertragspartei verschiedener internationaler Menschenrechtsverträge und Konventionen obliegt es der Schweiz, den internationalen Kontrollorganen regelmässig über die Umsetzung ihrer völkerrechtlichen Verpflichtungen Bericht zu erstatten. Auch unter diesem Aspekt leistet die Verabschiedung der hier vorgeschlagenen Mitteln und Massnahmen einen wichtigen Beitrag zum Kampf gegen Terrorismus und weitere gravierende Gefährdungen der internationalen Sicherheit, was dem Ansehen der Schweiz im internationalen Umfeld förderlich ist.

Der vorliegende Gesetzesentwurf steht sowohl in Bezug auf seine allgemeine Zielrichtung wie auch hinsichtlich der einzelnen Bestimmungen im Einklang mit der EMRK und dem Internationalen Pakt vom 16. Dezember 1966[69] über bürgerliche und politische Recht (Pakt II).

Gemäss EMRK kann die Ausübung grundlegender Rechte (wie beispielsweise die Achtung des Privat- und Familienlebens nach Art. 8 oder die Versammlungsfreiheit nach Art. 11 EMRK) eingeschränkt werden, wenn die Einschränkung gesetzlich vorgesehen ist, ein legitimes Ziel verfolgt und in einer demokratischen Gesellschaft notwendig sind. Das vorliegende Revisionspaket erfüllt die Voraussetzungen an ein Gesetz im materiellen Sinne gemäss EMRK. Insbesondere legen die neuen Bestimmungen den betroffenen Personenkreis (vgl. insbesondere Art. 18*k*–18*n*), die Anwendungsvoraussetzungen (vgl. insbesondere Art. 18*a* und 18*b*) und die Verfah-

69 SR **0.103.2**

rensgarantien (vgl. insbesondere Art. 18*d*, 18*e*, 18*f* und 18*i*) mit hinreichender Bestimmtheit fest. Die Prüfung der zwei übrigen Voraussetzungen (legitimes Ziel, Notwendigkeit in einer demokratischen Gesellschaft) entspricht derjenigen des öffentlichen Interesses und der Verhältnismässigkeit (vgl. oben).

Der Pakt II garantiert in Bezug auf die vorliegend zur Diskussion stehenden Grundrechte (vgl. Art. 17 bzw. Art. 22 Pakt II) keinen weitergehenden Schutz als die EMRK oder die BV.

Im Übrigen sind die vorgeschlagenen Mittel mit den spezifisch auf Terrorismus zugeschnittenen Abkommen und Vereinbarungen ohne weiteres kompatibel.

5.3 Erlassform

5.3.1 Gesetzesform

Wichtige rechtsetzende Bestimmungen über die Einschränkung verfassungsmässiger Rechte müssen als Bundesgesetz ergehen (Art. 36 Abs. 1, 163 Abs. 1 und 164 Abs. 1 BV). Diese Voraussetzungen sind vorliegend erfüllt.

5.3.2 Teilrevision

Obwohl eine Totalrevision vor allem aus Übersichtlichkeitsgründen wünschenswert wäre, wurde aus folgenden Gründen einer Teilrevision der Vorzug gegeben:

- Zur Zeit ist noch offen, was mit den im Rahmen von BWIS I (Bekämpfung von Gewalt an Sportveranstaltungen) befristet beschlossenen Regelungen nach Ablauf ihrer Geltungsfrist (2009) geschehen wird.
- Die im Rahmen der vorliegenden Gesetzesrevision angestrebten Änderungen enthalten zwar zahlenmässig vergleichsweise viele Gesetzesartikel, beschränken sich aber in materieller Hinsicht auf wenige Themen mit dem klaren Schwerpunkt der Informationsbeschaffung mit besonderen Mitteln.
- Die angestrebten Änderungen lassen sich gesetzessystematisch zwar nicht ideal, aber in vertretbarer Weise in die bestehende Gliederung integrieren.

5.4 Unterstellung unter die Ausgabenbremse

Nach Artikel 159 Absatz 3 Buchstabe b BV bedarf das Gesetzgebungspaket der Zustimmung der Mehrheit beider Räte, wenn der Beschluss neue wiederkehrende Ausgaben von mehr als 2 Millionen Franken nach sich zieht. Diese Voraussetzung ist vorliegend zwar erfüllt, doch wird der Stellen- und Finanzbedarf mit einer departementsinternen Kompensation gedeckt.

5.5 Vereinbarkeit mit dem Subventionsgesetz

Die einhellige Forderung der Kantone in der Vernehmlassung geht dahin, dass der Bund ihnen allfällige zusätzliche Aufwendungen im Staatsschutz abzugelten habe.

Artikel 28 Absatz 1 BWIS regelt die finanziellen Leistungen an die Kantone wie folgt: Der Bund gilt den Kantonen die in seinem Auftrag nach dem dritten Abschnitt erbrachten Leistungen ab. Der Bundesrat legt die Abgeltung aufgrund der Zahl der überwiegend für die Bundesaufgaben tätigen Personen pauschal fest.

In den dazugehörigen Erläuterungen wurde dargelegt, dass bei der Informationsbearbeitung eine Nichtübernahme der Kosten fatale Auswirkungen haben könnte, weshalb sich eine Abweichung vom Grundsatz rechtfertige, wonach die Kantone die Kosten des Vollzugs von Bundesrecht selber zu tragen hätten. Diese Ausführungen beanspruchen nach wie vor Gültigkeit.

5.6 Delegation von Rechtsetzungsbefugnissen

Nach Artikel 10*a* des vorliegenden Entwurfs regelt der Bundesrat beim elektronischen Lage- und Führungsinformationssystem die Zugriffsrechte im Einzelnen und die Grundsätze für die Aufbewahrung und Löschung der Daten. Sodann bestimmt er die nach Artikel 13*a* des Entwurfs zur Auskunft verpflichteten Organisationen in einer Verordnung und legt nach Artikel 14*a* des Entwurfs die Tätigkeiten, die Organisation und das Verfahren der Funkaufklärung im Einzelnen fest. Zudem regelt er gemäss Artikel 99*a* MG die Zusammensetzung der unabhängigen Kontrollinstanz, die Entschädigung ihrer Mitglieder und die Organisation ihres Sekretariates.

Rechtsvergleich (Deutschland, Österreich, Frankreich, Italien, Luxemburg, Niederlande, EU)

1. Deutschland

Die Bundesrepublik Deutschland ist ein Bundesstaat und föderalistisch organisiert. Die föderale Verfassungsordnung Deutschlands weist den Ländern grundsätzlich die Polizeihoheit auf ihrem jeweiligen Staatsgebiet zu.

Hauptaufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist die Sammlung und Auswertung von Informationen über die Bestrebungen, welche sich gegen die freiheitliche demokratische Grundordnung richten, sowie sicherheitsgefährdende oder geheimdienstliche Tätigkeiten und Bestrebungen im Geltungsbereich des Bundesverfassungsschutzgesetztes.[70]

Der Bund und die Länder sind in Angelegenheiten des Verfassungsschutzes zur Zusammenarbeit verpflichtet. Der Bund unterhält ein Bundesamt für Verfassungsschutz (BfV), welches dem Bundesminister des Innern untersteht. Das BfV darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschliesslich personenbezogener Daten verarbeiten und nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen im BVerfSchG entgegenstehen. Zusätzlich kann es Daten und Informationen von den repressiven Behörden beziehen.[71] Umgekehrt darf der Bundesnachrichtendienst Informationen an inländische Behörden übermitteln, wenn dies zur Erfüllung seiner aufgaben erforderlich ist oder wenn die Daten für Zwecke der öffentlichen Sicherheit benötigt werden.[72] Diese Daten dürfen für Strafverfolgungszwecke verwendet werden.

Die Tätigkeiten des BfV unterliegen der Kontrolle durch ein Parlamentarisches Kontrollgremium, welches regelmässig über die allgemeine Tätigkeit des BfV und über Vorgänge von besonderer Bedeutung zu unterrichten ist.[73] Die Bundesregierung hat dem Parlamentarischen Kontrollgremium auf Verlangen Einsicht in den Akten und Dateien zu geben und die Anhörung von Mitarbeitern zu gestatten. Das BfV ist verpflichtet, Betroffenen auf Antrag unentgeltlich Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen, soweit er hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt.[74] Die gespeicherten Daten müssen berichtigt werden, sofern sie unrichtig sind. Spätestens nach fünf Jahren muss das BfV bei der Einzelfallbearbeitung prüfen, ob die Daten zu berichtigen oder zu löschen sind. Spätestens 15 Jahre nach dem Zeitpunkt der

70 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz; BVerfSchG).
71 § 18 BVerfSchG
72 § 9 Gesetz über den Bundesnachrichtendienst vom 20. Dezember 1990 (BNDG)
73 § 2 Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes
74 § 15 BVerfSchG

letzten Speicherung sind die Informationen zu löschen, ausser bei abweichender Entscheidung der Behördenleiter.[75]

Nachfolgend werden die Bestimmungen des Bundes erläutert.

Im Einzelfall darf das BfV zur Erfüllung seiner Aufgaben u.a. Telekommunikationsdaten und Teledienstleistungen einholen[76]. Der Antrag ist durch den Präsidenten des BfV oder seinen Vertreter schriftlich zu stellen und zu begründen. Über den Antrag entscheidet das vom Bundeskanzler beauftragte Bundesministerium. Dieses unterrichtet monatlich die G 10-Kommission über die beschiedenen Anträge vor deren Vollzug. Bei Gefahr in Verzuge kann das Bundesministerium den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen.[77] Das zuständige Bundesministerium unterrichtet im Abstand von höchstens sechs Monaten das Parlamentarische Kontrollgremium (PKGr) über die Durchführung der Informationsbeschaffungen. Weiter ist das BfV zum Einsatz von Vertrauensleuten und Gewährspersonen befugt sowie Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anzuwenden.[78] Diese Massnahmen sind in einer Dienstvorschrift zu benennen, welche wiederum der Zustimmung des Bundesministers des Innern bedarf. Dieses unterrichtet das parlamentarische Kontrollgremium. Werden Auskünfte beim Betroffenen eingeholt, so muss der Erhebungszweck angegeben werden.

Das BfV ist des Weiteren unter bestimmten Voraussetzungen befugt, Auskünfte bei Banken einzuholen.[79] Auch darf das BfV, wenn es Informationen über Kommunikationswege terroristischer Gruppen benötigt, von den Erbringern von Postdienstleistungen Auskünfte wie z.B. Namen, Adressen und Angaben zu Postfächern einholen sowie Telekommunikationsverbindungsdaten wie Kennungen, Rufnummern und Daten über Standorte.[80] Schliesslich darf das BfV Geräte zur Ermittlung der Geräte- und Kartennummern von mobilen Telefonen einsetzen.[81] Es gelten dabei die gleichen Voraussetzungen wie bei den Telefonabhörungen.

Dagegen stehen den Verfassungsschutzbehörden Deutschlands keinerlei polizeiliche Befugnisse zu, namentlich dürfen keine Durchsuchungen durchgeführt und keine Gegenstände beschlagnahmt werden.

Im Nachgang zu den Anschlägen vom 11. September 2001 wurde das befristete Terrorismusbekämpfungsgesetz (TBGE)[82] am 12. Juli 2006 revidiert und vom Bundeskabinett als Terrorismusbekämpfungsergänzungsgesetz (TBEG)[83] umgesetzt. Die Nachrichtendienste können neu automatisiert Auskünfte aus dem zentralen Fahrzeugregister abrufen. Auch ist zur Abwehr von erheblichen Gefahren die europaweite Ausschreibung von Verdächtigen zur verdeckten Registrierung möglich. Die Dienste werden informiert, wenn die ausgeschriebene Person in eine Polizeikontrolle gerät. Neu können sich die Auskunftsersuchen auch auf verfassungsfeindliche

75 § 12 BVerfSchG
76 § 8 Abs. 8 BVerfSchG
77 § 8 Abs. 9 BVerfSchG
78 § 8 Abs. 2 BVerfSchG
79 § 8 Abs. 5 BVerfSchG
80 § 8 Abs. 6 BVerfSchG und § 8 Abs. 8 BVerfschG
81 § 9 Abs. 4 BVerfSchG
82 Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBI I 2002, S. 361, 3142)
83 Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5. Januar 2007 (BGBI I 2007, 2)

Bestrebungen erstrecken. Die sensiblen nachrichtendienstbezogenen Regelungen sind auf fünf Jahre befristet und sollen vor Ablauf evaluiert werden.

2. Österreich

Das österreichische Staatssystem ist föderalistisch organisiert. Ihre Rechtsordnung macht grundsätzlich einen Unterschied zwischen dem repressivem und dem präventiven Bereich. Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) nimmt die Aufgaben des zivilen Nachrichtendiensts Österreich wahr.[84] Die Aufgaben des BVT sind im Wesentlichen der Schutz des Staates und seiner verfassungsmässigen Einrichtungen. Zu seinen Kernaufgaben zählen die Bekämpfung des internationalen Terrorismus, extremistischer Phänomene, der Spionage, des internationalen Waffenhandels, des Handels mit Kernmaterial und der organisierten Kriminalität in diesen Bereichen. Das BVT ist Teil der Generaldirektion für die öffentliche Sicherheit im Bundesministerium für Inneres.

Jedes Bundesland verfügt für die Aufgabenerfüllung im Bereich Verfassungsschutz über ein Landesamt für Verfassungsschutz und Terrorismusbekämpfung, welches Teil der jeweiligen Sicherheitsdirektion ist. Darüber hinaus obliegt dem BVT die Veranlassung und Koordination und via der LVT auch die Umsetzung von Personen- und Objektschutzmassnahmen sowie der Schutz von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte.

Den Staatsschutzbehörden ist der Zugriff auf Daten der repressiven Behörden gestattet. Letztere liefern ihre Informationen an die Staatsschutzbehörden weiter. Die Betroffenen haben das Recht auf Auskunft, Richtigstellung oder Löschung personenbezogener Daten und Möglichkeit der Beschwerde an die Datenschutzkommission. Wenn Staatsschutzinteressen es erfordern, kann ausnahmsweise die Auskunft verweigert werden.

Die Sicherheitsbehörden, welche die erweiterte Gefahrenerforschung ausüben, haben unverzüglich den Bundesminister für Inneres über die von ihnen ergriffenen Massnahmen zu verständigen. Ermittlungen dürfen in diesem Rahmen erst nach Mitsprache des Rechtsschutzbeauftragten oder nach Ablauf einer drei Tagesfrist erfolgen, ausser die sofortige Ermittlung ist zur Abwehr einer schweren Gefahr erforderlich.[85]

Nimmt der Rechtsschutzbeauftragte wahr, dass durch das Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenanwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus Gründen nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzkommission befugt.

Über die Tätigkeiten im Rahmen der erweiterten Gefahrenerforschung (Beobachtung von Gruppierungen) hat der Rechtsschutzbeauftragte dem Bundesminister für Inneres jährlich zu berichten[86]. Dieser hat den Bericht dem ständigen Unterausschuss des Nationalrates auf dessen Verlangen zugänglich zu machen.

84 Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei vom 31. Oktober 1992 (Sicherheitspolizeigesetz; SPG).
85 § 62*a* Abs. 7 SPG (SPG Novelle 2005)
86 § 21 Abs. 3 SPG

Die Staatsschutzbehörden sind ermächtigt, von den Betreibern öffentlicher Telekommunikationsdienste unter bestimmten Voraussetzungen Auskünfte einzuholen. Die Post- und Fernmeldeüberwachung ist jedoch nur den repressiven Behörden gestattet. Auch kann verdeckt ermittelt und dabei eine Tonaufnahme hergestellt werden.[87] Die Tonaufnahme ohne gleichzeitige Anwesenheit des verdeckten Ermittlers ist unzulässig. Dem Rechtsschutzbeauftragten obliegt die begleitende Kontrolle der verdeckten Ermittlung und des verdeckten Einsatzes von Bild- und Tonaufzeichnungsgeräten.[88] Über solche Ermittlungen ist der Rechtsschutzbeauftragte mit Angabe der für die Ermittlungen wesentlichen Gründe in Kenntnis zu setzen, soweit die Identität der Betroffenen bekannt ist. Den Staatsschutzbehörden ist des Weiteren die Sicherstellung, Beschlagnahmung, Einziehung[89], das Observieren[90] und Betreten von privaten Räumen[91] gestattet, sowie die Anordnung und Durchführung von Befragungen.[92] Finanzintermediäre sind in bestimmten Fällen verpflichtet, Auskünfte den zuständigen Behörden zu übermitteln.[93]

Die Tätigkeit des BTV unterliegt der parlamentarischen Kontrolle gemäss Artikel 52*a* B-VG. Nach Erschöpfung des administrativen Instanzenzuges kann beim Verwaltungs- oder Verfassungsgerichtshof Beschwerde erhoben werden.

Auch in Österreich blieb der 11. September 2001 nicht ohne Folgen. Die Strukturen sind gestrafft und die Gesetzesbestimmungen verschärft worden. Im Zuge dieser Verschärfung haben die Staatschutzbehörden weiter reichende Kompetenzen erhalten.

Durch die Sicherheitspolizeigesetz-Novelle 2002 erfolgte eine Ausdehnung des Schutzes von Menschen, die über einen gefährlichen Angriff oder eine kriminelle Verbindung Auskunft erteilen können, auch auf Angehörige dieser Personengruppe Die rechtlichen Grundlagen für die Tarnung von Unterstützungsmassnahmen bei der Durchführung von Observationen oder verdeckten Ermittlungen wurden ebenfalls geändert. Vor dem Hintergrund extremistischer Entwicklungen wurden am 1. Oktober 2000 Bestimmungen über die erweiterte Gefahrenerforschung mit den entsprechenden Rechtsschutzregelungen in das SPG aufgenommen.[94] Mit diesen Bestimmungen ist den Sicherheitsbehörden nun die Beobachtung von Gruppierungen möglich, wenn damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität kommen könnte. Davor waren die Sicherheitsbehörden erst dann zur Beobachtung von extremistischen Gruppierungen ermächtigt, wenn diese bereits kriminell agierten.

Mit Sicherheitspolizeigesetz-Novelle vom Dezember 2003 wurde die Sicherheitsbedenklichkeitsbescheinigung für Unternehmungen und Anlagen eingeführt.[95]

Am 1. Dezember 2002 wurden im Bundesministerium für Inneres das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung eingerichtet.[96] Es ist dem Generaldirektor für die öffentliche Sicherheit unmittelbarer unterstellt.

87 § 54 SPG
88 § 62*a* Abs. 7 SPG
89 § 42 SPG
90 § 54 Abs. 2 SPG
91 § 39 SPG
92 § 28*a* SPG
93 § 38 Bankwesengesetz (BWG)
94 § 21 Abs. 3, 53 Abs. 1 Z. 2a, 54 Abs. 2 und 62*a* SPG
95 § 55–55*b* SPG
96 § 7 Abs. 1 und 9 Bundesministeriengesetz

Dieses übt seine Tätigkeit im Rahmen des Sicherheitspolizeigesetzes (SPG) und, soweit es im Dienste der Strafjustiz tätig wird, nach den Bestimmungen der Strafprozessordnung (StPO) aus.

3. Frankreich

Frankreich ist eine zentralistisch organisierte Demokratie. Die 26 Regionen verfügen im Gegensatz zu den Schweizer Kantonen über keine eigentliche Autonomie.

Der Premierminister ist direkt für die innere Sicherheit zuständig, wobei er vom Generalsekretariat für nationale Verteidigung (SGDN)[97] und von einem Militärkabinett unterstützt wird. Mit der inneren Sicherheit sind verschiedene Staatsdienste befasst. Infolgedessen besteht keine eigentliche Trennung von Prävention und Repression.

Frankreich besitzt zwei unabhängige Sicherheitsdienste: Die Polizei und die Gendarmerie Nationale. Die Gendarmerie ist für alle ländlichen Regionen zuständig ist, die Polizei für die Stadtgebiete. Die mobile Gendarmerie ist für die Aufrechterhaltung der öffentlichen Ordnung sowie die Bekämpfung des Terrorismus, des organisierten Verbrechens und der Sekten zuständig. Die nationale Polizei untersteht dem Innenministerium und wird von der Generaldirektion der nationalen Polizei (DGPN)[98] geleitet. Sie vereint zahlreiche Subdirektionen unter ihrem Dach, u.a. die Direktion des Inlandsgeheimdienstes (D.S.T.)[99], die Zentraldirektion des Verfassungsschutzes (DCRG)[100] und die Koordinationsstelle für Terrorismusbekämpfung.[101]

Die D.S.T. nimmt die Stellung eines Nachrichtendienstes ein und hat den Auftrag, die Verbrechen gegen die Sicherheit des Staates zu bekämpfen.[102] Ihre genaue Organisation und die Funktion sind in einem geheimen Beschluss vom 8. März 1993 geregelt. Die D.S.T. als zentrale Stelle sammelt und bearbeitet sämtliche Informationen, die ihr von den RG übermittelt werden und sorgt für deren Weitergabe. Zudem beteiligt sich die D.S.T. am Schutz sensibler Bereiche und Geheimnisse der Landesverteidigung. Die RG betreiben ein Informationssystem, zu welchem auch die D.S.T. Zugriff hat.[103]

Die Koordinationsstelle für Terrorismusbekämpfung koordiniert die Arbeit aller Dienste, die im In- und Ausland mobilisiert sind.

Das SGDN ist eine interministerielle Behörde und ist u.a. für die Sicherheit der Informationssysteme, für die Terrorprävention- und Abwehr, für die Absicherung der Steuerungs- und Kommunikationsstrukturen der Regierung und Bekämpfung der Proliferation von Atomwaffen verantwortlich und überwacht die Ausfuhr von Kriegsmaterial.

97 Secrétariat Générale de la Défense Nationale
98 Direction Générale de la Police Nationale
99 Direction de la surveillance du territoire
100 Renseignements généraux
101 Unité de coordination de la lutte antiterroriste
102 Dekret Nr. 82-1100 vom 22. Dezember 1982, aktualisiert am 15. September 2004
103 Dekrete Nr. 91-1052 und NR 91-1051

Die Generaldirektion für äussere Sicherheit (DGSE)[104] ist dagegen ist als Auslandsgeheimdienst für die äussere Sicherheit Frankreichs zuständig. Diese untersteht dem Premierminister und ist mit der Informationsbeschaffung und Intervention befasst.

Die Einsichtsrechte in die Informationssysteme der RG erfolgen in der Regel nach dem so genannten indirekten Verfahren.[105] Das Einsichtsgesuch muss bei der unabhängigen «Commission nationale de l'information et des libértés» (CNIL) eingereicht werden. Diese überprüft die Informationen und orientiert den Gesuchsteller, falls Berichtigungen vorgenommen wurden. Wenn die innere Sicherheit nicht gefährdet ist, können die Daten dem Gesuchsteller mitgeteilt werden. Falls die Datenbank Informationen umfasst, deren Bekanntgabe an die betroffene Person den Zweck der Datenbank nicht gefährdet, kann der Verantwortliche der Datenbank dem Betroffenen direkt informieren.

Es können präventive Telefonüberwachungen im Interesse der inneren Sicherheit angeordnet werden zum volkswirtschaftlichen Schutz Frankreichs, für die Terrorprävention und Bekämpfung der organisierten Kriminalität und bei rechtswidrigen Gruppierungen.[106] Gemäss Artikel 4 des Gesetzes vom 10. Juli 1991 wird die Bewilligung durch Beschluss des Premierministers oder zweier durch ihn ernannter Personen erteilt, auf Antrag des Verteidigungsministers, des Innenministers und des Ministers für Zollwesen oder ihrer Stellvertreter. Die Zahl der gleichzeitig vollziehbaren angeordneten Massnahmen sind durch den Premierminister mittels Kontingenten begrenzt und wird durch eine verwaltungsunabhängige «Commission nationale de contrôle des interceptions de sécurité» überwacht.[107] Diese besteht aus einem Präsidenten, welcher für eine Dauer von 6 Jahren durch den Präsidenten der Republik gewählt wird und weiteren Personen. Die Bewilligung wird höchstens für 4 Monate erteilt und kann unter den gleichen Bedingungen jeweils für höchstens weitere 4 Monate verlängert werden. Die gewonnen Erkenntnisse der Überwachung müssen spätestens nach 10 Tagen nach Ausführung unter Aufsicht des Premierministers zerstört werden.

Gemäss Kommission sind alle Informationen im Zusammenhang mit den präventiven Abhörungen als «Secret-Défense» zu klassifizieren. Das heisst u.a., dass Personen die präventiv abgehört wurden, nicht zu informieren sind, weil dies der «défense nationale» grosse Schäden zufügen könnte. Den Staatsschutzbehörden Frankreichs ist hingegen die Postüberwachung untersagt.

Es können des Weiteren in Ausnahmefällen per begründeten Beschluss Einziehungen vorgenommen und Wertgegenstände gesperrt werden, wenn die innere Sicherheit es erfordert[108]. Die Durchführung von Befragungen ist vorgesehen. Des Weiteren sind Durchsuchungen von Fahrzeugen und Hausdurchsuchungen ohne richterliche Prüfung erlaubt.[109] Bei organisierter Kriminalität sind Einätzte auch in der Nacht zugelassen.

104 Direction Générale de la Sécurité Extérieure
105 Loi pour la sécurité intérieure (LOI nº 2003-239 vom 18. März 2003; nachfolgend Gesetz vom 18. März 2003)
106 Art. 3 Gesetz Nr. 91-646 vom 10. Juli 1991 (Loi relative au secret des correspondances émises par la voie des télécommunications; nachfolgend Gesetz vom 10.Juli 1991)
107 Art. 5 Gesetz vom 10. Juli 1991
108 Art. 3 Gesetz vom 18. März 2003 und Gesetz Nr. 2005-750 vom 4. Juli 2005 (Loi nº 2005-750)
109 Gesetz Nr. 2004-204 vom 9. März 2004 (nachfolgend Gesetz vom 9. März 2004)

Was die verdeckten Bild- und Tonaufzeichnungen, Tarnpapieren und Tarnkennzeichen betrifft**,** wurden verschiedene Kompetenzen mit dem Gesetz vom 18. März 2003 begründet: Demnach sind beispielsweise direkte Zugriffe auf Informationssysteme und das Einholen von Auskünften bei Banken oder Privaten erlaubt. Betätigungsverboten können unter bestimmten Umständen ausgesprochen werden, namentlich bei bewaffneten Demonstrationen und bei Organisationen, welche die Sicherheit Frankreichs gefährden würden.[110] Im Rahmen der organisierten Kriminalität ist der Einsatz von Vertrauensleuten vorgesehen, mit nachträglicher Benachrichtigung des Staatsanwaltes. Für deren Abgeltung existieren Spezialfonds.[111]

Mit Gesetz vom 19. Januar 2006 wurde u.a. die Videoüberwachung in öffentlichen Gebäuden oder sensiblen Einrichtungen bei einer möglichen Gefährdung durch terroristische Akte ausgeweitet, der Zugriff für die Polizei oder die Gendarmerie Nationale auf die elektronischen Daten der Anbieterinnen von Fernmeldediensten und von Fluggesellschaften gestattet, eine Verlängerung der Polizeihaft ermöglicht sowie eine Kontrollmöglichkeit in internationalen Zügen eingeführt.[112]

In Frankreich ist kein parlamentarisches Kontrollsystem vorgesehen, jedoch sind diesbezüglich verschiedene Gesetzesprojekte in Bearbeitung**.** Indessen muss die Regierung dem Parlament Rechenschaftsberichte abliefern.

4. Italien

Italien ist im Gegensatz zu den Bundesstaaten Schweiz, Deutschland, oder Österreich ein dezentralisierter Einheitsstaat.

Die Wahrung der inneren und äusseren Sicherheit ist in Italien auf drei Pfeiler aufgebaut: Den SISMI (Servizio per le informazioni e la sicurezza militare), den SISDE (Servizio per le informazioni e la sicurezza democratica) und die Direzione Investigativa Antimafia (D.I.A.).

Deren Wahrung liegt in der Zuständigkeit des Innenministeriums. Ihm unterstellt ist die «Direzione centrale per la Polizia di Prevenzione».[113]

Die «Polizia di Prevenzione» hat folgende Zielsetzungen: die Bekämpfung von internen und externen Terrororganisationen und von paramilitärischen und gewalttätigen Gruppierungen. So können aufgrund von Artikel 6 des Gesetzes 121 Daten klassifiziert, analysiert und evaluiert werden, um die Sicherheit zu gewährleisten.

Während der SISMI für die Aktivitäten zuständig ist, die im Ausland stattfinden, ist es der SISDE für die im Inland. Zu den Aufgaben des SISDE gehören die Bekämpfung von Terrorismus, illegaler Einwanderung, Computerkriminalität, Wirtschaftsspionage, neu aufkommender Bedrohungen und organisierter Kriminalität.

Die SISDE sammelt Daten zum Schutz der inneren Sicherheit. Grundsätzlich besteht ein Einsichtsrecht.[114] Alle Dokumente und Akten, deren Veröffentlichung die

110 Gesetz vom 10 Januar 1936
111 Gesetz vom 9. März 2004
112 Gesetz Nr. 2005-532 vom 19. Januar 2006 (Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers; nachfolgend Gesetz vom 19. Januar 2006)
113 Gesetz «legge n. 121 del 1981 Nuovo ordinamento dell'Amministrazione della pubblica sicurezza»; nachfolgend Gesetz 121
114 «Decreto legislative del 30 giugno 2003, n. 196», nachfolgend Dekret 196

Sicherheit des Staates gefährden würde, unterstehen jedoch dem Staatsgeheimnis.[115] Der Datenschützer (Garante per la protezione dei dati personali) übt die Kontrolle über die gesammelten Daten aus. Die Staatsschutzbehörden arbeiten im Rahmen der Informatiksicherheit mit den Behörden der Kriminalpolizei zusammen.

Die Aktivitäten der SISMI und SISDE werden von einer parlamentarischen Kommission überwacht. Die Regierung muss dem Parlament pro Semester ein Rechenschaftsbericht über die Aktivitäten der Dienste abliefern. Auch sind die Aktivitäten der Nachrichtendienste der Kontrolle der Justiz unterstellt.

Die «Direzione Investigativa Antimafia» (D.I.A.) führt Massnahmen gegen die organisierte Kriminalität durch, wie Überwachungen, u.a. auch telefonische Überwachungen und ermittelt gegen die Mafia.[116] Sie kann Informationen beschaffen betreffend finanzielle Verhältnisse der Personen, die verdächtigt werden, kriminellen Organisationen anzugehören. Die D.I.A. gibt die gesammelten Informationen an die SISDE und SISMI weiter. Zudem arbeitet die D.I.A. mit den Polizeikräften zusammen.

Grundsätzlich dürfen Daten nur mit Einverständnis der Betroffenen bearbeitet werden, ausser wenn die Datenbearbeitung aufgrund eines gesetzlichen Auftrages erfolgt.[117]

Aufgrund des Gesetzesdekretes vom 27. Juli 2005 sind eine Reihe von zusätzlichen weiteren Kompetenzen und Massnahmen für die Staatschutzbehörden eingeführt worden:[118] Neu sind bei begründetem Terrorverdacht oder bei Gefährdung der Staatsordnung präventive Telefonüberwachungen möglich. Der Antrag ist in der Regel im Voraus durch den Ministerpräsidenten zu begründen. Dieser kann seine Befugnisse an die Nachrichtendienste delegieren. Die Anordnung erfolgt unter Einwilligung des Richters durch die Staatsanwaltschaft. Ist Gefahr in Verzug, kann auch ohne richterliche Einwilligung angeordnet werden. Spätestens nach 24 Stunden muss beim Richter auf dem ordentlichen Weg aber die Bewilligung eingeholt werden. Der Richter muss innerhalb von 48 Stunden über den Antrag entscheiden. Falls diese Frist nicht eingehalten werden kann, so sind die gewonnenen Erkenntnisse nicht gerichtsverwertbar.

Des Weiteren wurde mit dem bis Ende Dezember 2007 befristeten Gesetz 675 die Pflicht zur Aufbewahrung von Telefon- und Internetdaten für die Telekommunikationsgesellschaft und Internetprovider eingeführt. Das Verhör von Gefangenen ohne Anwesenheit eines Verteidigers (colloquio investigativo), welches bislang auf Mafia-Delikte beschränkt war, ist nun den Staatsschutzbehörden gestattet.

Schliesslich wurde die Möglichkeit der erleichterten Ausschaffung von Verdächtigen geschaffen, die eine Gefahr für die öffentliche Sicherheit darstellen oder in irgendeiner Art eine terroristische Organisation unterstützen. Die Ausschaffung wird unverzüglich vollzogen, kann aber vor dem Verwaltungsgericht angefochten werden. Stützt sich der Ausschaffungsentscheid auf geheimdienstliche Quellen, so kann die Gerichtsverhandlung um zwei Jahre aufgeschoben werden. Die Ausschaffungsverfügung kann suspendiert werden, wenn der Auszuschaffende mit den Behörden

115 Art. 12 Gesetz vom 24. Oktober 1997
116 «legge n. 410 del 1991»; nachfolgend Gesetz 410
117 Art. 12 Abs. 1 «legge n. 675 del 31 dicembre 1996 Tutella delle persone e di altri soggetti rispetto al trattamento die dati personali», nachfolgend Gesetz 675 genannt
118 Testo del decreto-legge 27 luglio, n.144, coordinato con la legge die conversione 31 luglio 2005 (nachfolgend Gesetz vom 27. Juli 2005)

kooperiert. Im Fall einer für die Ermittlungen massgeblichen Kooperation in Terrorismusermittlungen kann eine Niederlassungsbewilligung gewährt werden.

Bei Missbrauch kann die Bewilligung wieder entzogen werden.

Mit dem Gesetz vom 27. Juli 2005 wurde für das Innenministerium schliesslich die Möglichkeit zur Einrichtung von polizeicorpsübergreifenden Anti-Terrorismuseinheiten (unità investigative interforze) geschaffen.

5. Luxemburg

Luxemburg ist eine konstitutionelle Monarchie in Form einer parlamentarischen Demokratie und in drei Distrikte mit zwölf Kantonen und 118 Gemeinden gegliedert.

In Luxemburg sind drei Institutionen mit dem präventiven Staatsschutz befasst. Der für die innere Sicherheit zuständige zivile Nachrichtendienst (SRDE)[119], ferner der zivile Nachrichtendienst, zuständig für die äussere Sicherheit (HCSE)[120] und der militärische Nachrichtendienst.[121] Der SRDE ist dem Innenministerium unterstellt.

Die Kompetenzbereiche des SRDE sind einerseits die Bekämpfung des Terrorismus, der Spionage, der Proliferation von nicht konventionellen Waffen und damit betreffenden Technologien und der organisierten Kriminalität in diesem Geltungsbereich. Andererseits sind es alle Aktivitäten, welche die Integrität, die Souveränität und die Unabhängigkeit des Landes, die Sicherheit der Institutionen und das Funktionieren des Staates oder die Sicherheit des Volkes gefährden können.[122] Im Rahmen ihrer Befugnisse arbeitet der SRDE einerseits mit den polizeilichen-, den gerichtlichen Behörden und mit der Verwaltung und andererseits mit dem HCSE zusammen. Die Polizei und Gerichtsbehörden sowie die Verwaltung sind ihrerseits verpflichtet, Informationen im Geltungsbereich von Artikel 2 des Organisationsgesetzes vom 15. Juni 2004 an den SRDE weiterzuleiten.

Die Bearbeitung von Personendaten durch den SRDE richtet sich nach den Bestimmungen des «Loi du 2 août 2002».[123] Der SRDE hat Zugriff zu einer begrenzten Anzahl von Datenbanken, namentlich zur allgemeinen Polizeidatenbank, zur Ausländerdatenbank der Fremdenpolizei und zur Verkehrsdatenbank[124]. Die Aufsichtskontrolle wird durch den Generalstaatsanwalt oder einer seiner Delegierten wahrgenommen und zwei vom Minister gewählten Vertreter einer Spezialkommission. Diese haben Zugang zu den bearbeiteten Daten des SRDE, veranlassen die nötigen Berichtigungen und informieren die betroffenen Personen darüber, dass von ihnen gesetzeskonform Informationen über sie bearbeitet werden.

Bei Belangen der organisierten Kriminalität und der äusseren .Sicherheit[125] kann der Regierungspräsident auf Antrag des SRDE und im Einverständnis mit einer Spezial-

119 «le Sevice de Renseignement de l'Etat»
120 «La Haute Commissariat de la Sécurité Extérieure»
121 «2e Bureau de l'Armée».
122 «Loi du 15 juin portant organisation du Service de Renseignement de l'Etat» (nachfolgend Organisationsgesetz vom 15. Juni 2004)
123 «Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel» (nachfolgend Gesetz vom 2. August 2002)
124 Art. 4 des Organisationsgesetzes vom 15. Juni 2004
125 «Sécurité exterieure de l'Etat»

kommission präventive Telefonüberwachungen anordnen.[126] Die Überwachung muss nach drei Monaten eingestellt werden, kann aber jeweils um weitere drei Monate verlängert werden. Erkenntnisse, die im Rahmen einer Telefonüberwachung gewonnen worden sind, sind gerichtlich nicht verwertbar, wenn die betreffende Person ein Berufsgeheimnisträger im Sinne von Artikel 458 des Code pénale ist und sie nicht in Verdacht steht, eine strafbare Handlung begangen zu haben oder eine solche zu planen. Der Chef des SRDE muss in diesem Fall die entsprechenden Unterlagen sofort vernichten. Die Beschlüsse der Kommission müssen an den jeweiligen Direktor der Telekommunikationsdienste weitergeleitet werden, welcher sodann die Abhörungen durch eine dafür geschaffene Stelle vollziehen und kontrollieren lässt. Nach Beendigung der Massnahmen erhalten die Betroffenen die kopierten Unterlagen der gewonnenen Erkenntnisse, sofern diese nicht als geheim klassifiziert worden sind. Werden während der fraglichen Zeit keine Resultate erzielt, müssen sämtliche Unterlagen vernichtet werden, ansonsten erst nach Beendigung des Verfahrens.

Die Aktivitäten des SRDE sind der Kontrolle der Kommission unterstellt, welche sich aus Vorsitzenden der im «Chambre des Députés» vertretenen politischen Gruppen zusammensetzt. Der Direktor des Nachrichtendienstes informiert über die allgemeinen Aktivitäten seines Dienstes. Die Kommission kann Einsicht in die Dossiers verlangen und die mit den Dossiers befassten Agenten befragen. Sie verabschiedet einen an den Premierminister, den Chef des Nachrichtendienstes und die Deputierten der Kontrollkommission adressierten vertraulichen Schlussbericht, welcher auch die Observationen, Schlussfolgerungen und Empfehlungen beinhaltet. Die parlamentarische Kontrollkommission wird alle sechs Monate über die durchgeführten Massnahmen betreffend die präventive Telefonüberwachung informiert.

Es können weder Einziehungen und Durchsuchungen durchgeführt werden noch sind Zeugenbefragungen vorgesehen. Der Premierminister kann unter Einsatz von angemessenen technischen Mitteln die Überwachung jeglicher Form der Kommunikation anordnen, wenn der Verdacht besteht, dass die Sicherheit des Staates gefährdet sei.[127] Die auf diese Weise gesammelten Informationen dürfen den zuständigen Stellen nur beschränkt weitergegeben werden; nämlich nur der Name, Vorname und wenn vorhanden IP-Adresse.[128] Betätigungsverbote können nicht ausgesprochen werden.

Es sind verschiedene Gesetzgebungsprojekte in Vorbereitung, so Änderungen des Code-Pénal betreffend die Observationen und die Infiltration und bezüglich des «traitement d'informations de police générale (POLIS)».[129]

126 Art. 88-3 des Code- Pénal und nach dem «Loi du 26 novembre1982»
127 Art. 88-3 des «Code de procédure criminelle»
128 Loi du 30 mai 2005 relative à la protection de la personne à l'égard du traitement de données à caractère personnel dans le secteur de communications électroniques
129 Änderungen vom 17. März 2006 und vom 26. Mai 2006

6. Niederlande

Die Niederlande ist eine konstitutionelle Monarchie. Die Königin ist Mitglied der Regierung und ernennt die Minister.

Zum niederländischen Nachrichtendienst gehören die folgenden Institutionen: Der zivile Nachrichtendienst (AIVD)[130], der militärische Nachrichtendienst, zu welchem der eigentliche militärische Nachrichtendienst zählt (MIVD)[131], der militärische Spezialdienst (BD)[132] und schliesslich der Anti-Terrordienst[133]. Die Zusammenarbeit zwischen dem AIVD und der Polizei ist seit den Anschlägen vom 11.09.01 stark intensiviert worden.

Die Bekämpfung des Terrorismus zählt zu den wichtigsten Aufgaben des zivilen AIVD.

Die AIVD und MIVD führen Ermittlungen sowie Sicherheitsüberprüfungen und Massnahmen gegen Organisationen und Personen durch, die im Verdacht stehen, eine Gefahr für die Sicherheit, die demokratische Ordnung oder andere wesentlichen Staatsinteressen darzustellen.[134] Sie arbeiten mit den Polizei- und Strafverfolgungsbehörden über die Staatsanwaltschaft zusammen, indem Informationen in Form eines Berichts weitergegeben werden. Der AIVD ist befugt, den regionalen Nachrichtendiensten (RID) und dem Spezialsicherheitsdienst der königlichen Militärpolizei zu beantragen, in seinem Auftrag tätig zu werden. Eine Revision des Code of Criminal Procedure soll Informationen des AIVD vor Gericht verwertbar werden lassen.[135]

Grundsätzlich haben Betroffene auf Verlangen Einsichtsrecht in die Daten, die in Zusammenhang mit den gegen sie getroffenen Massnahmen erhoben worden sind; der Quellenschutz bleibt jedoch gewahrt. Die Einsichtsrechte werden eingeschränkt, sofern die Offenlegung der Daten eine Gefährdung der inneren Sicherheit zur Folge hätte. Über das Nichteintreten muss die dafür zuständige Aufsichtskommission informiert werden.[136] Diese wacht über die Tätigkeit der Dienste und unterrichtet die zuständigen Minister.

Der AIVD und der MIVD sind ermächtigt, präventive Post- und Fernmeldeüberwachungen durchzuführen. Der Antrag erfolgt zum Voraus unter Bewilligung des Verteidigungsministers durch den Chef des AIVD und des MIVD und im Einverständnis des Innenministers. Ist Gefahr in Verzug, ist eine nachträgliche Genehmigung unter der Voraussetzung zulässig, dass diese so schnell wie möglich eingeholt wird.

Des Weiteren sind die Dienste bei schriftlicher Einwilligung des zuständigen Ministers ermächtigt, Observationen unter Einsatz von technischen Mitteln auszurichten. Die Observation und Durchsuchungen privater Räume sind in Absprache mit dem Innenminister oder dem Chef der Dienste erlaubt. Auch sind Einsätze unter einer

130 «Algemene Inlichtingen- en Veiligheidsdienst» (General Intelligence and Security Service)
131 «Inlichtingen- en Veiligheidsdienst» (Military Intelligence and Security Service)
132 «Koninklijke Marechaussee, Bijzondere Dienst en Veiligheid» (Military police Special section for intelligence and security)
133 «Bijzondere Bijstands Eenheid» (Special Help Union Anti-Terrorist Service).
134 «Act of 7 February 2002, providing for rule s relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002)»
135 Parliamentary documents II, 29 743
136 Supervisory committee

Tarnidentität vorgesehen und erlaubt Briefe Dritter zu öffnen, sofern das Bezirksgericht Den Haag einem Antrag des Chefs der Dienste entspricht. Das Eindringen in fremde EDV-Systeme ist ebenfalls gestattet, sofern der Innenminister oder der Chef der Dienste ihr Einverständnis abgeben. Dagegen hat es keine ausdrücklichen Regelungen für die Beschlagnahme, Einziehung und Sicherstellung von Gegenständen noch für Betätigungsverbote gegen Einzelpersonen oder Organisationen:

Der von der Regierung unabhängige «Nationaler Ombudsmann» wacht u.a. über die Tätigkeiten der Dienste. Sein Einflussbereich gegenüber den Diensten wurde aber mit einer Revision weiter eingeschränkt.[137] Die Dokumente der Dienste sind zwar einsehbar, können aber nicht kopiert werden.

Der zuständige Minister informiert die parlamentarische Aufsichtskommission regelmässig über die Tätigkeiten der Dienste.

7. EU

Bereits mit der Einführung des Europäischen Polizeiamts (Europol) am 26. Juli 1995, welches sich u.a. die Verhütung und Bekämpfung des Terrorismus zum Ziel gesetzt hat, war die Bekämpfung des Terrorismus ein Anliegen der EU.

Seit den Anschlägen vom 11. September 2001 in den USA verfolgt die EU eine gezielte Politik zur Terrorismusbekämpfung. Im Nachgang zu den Bombenanschlägen in London sprach sich die EU anlässlich eines Sondertreffens der europäischen Innen- und Justizminister in Brüssel für eine engere Zusammenarbeit der 25 EU-Staaten im Anti-Terror-Kampf aus. Es wurde eine bessere Zusammenarbeit von Polizei und Geheimdiensten über die Grenzen hinweg gefordert.

Am 21. September 2005 hat die EU-Kommission ein umfassendes Paket von 4 Massnahmen vorgestellt.

1. Vorschlag für eine Richtlinie über die Aufbewahrung von Verkehrsdaten durch Dienstanbieter:

   Der Vorschlag stellt auf die Harmonisierung der Pflichten für Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes im Zusammenhang mit Vorratsspeicherfristen von einem Jahr für Verkehrsdaten von Gesprächen im Fest- und Mobilfunknetz, bzw. von sechs Monaten für Verkehrsdaten, die sich auf die Nutzung des Internets beziehen, ab.

2. Finanzbeschluss über 7 Millionen Euro für ein Pilotprojekt auf dem Gebiet der Prävention, Abwehrbereitschaft und Reaktion im Zusammenhang mit Terroranschlägen:

   Der Finanzbeschluss stellt darauf ab, die Strafverfolgungsbeteiligten zu vernetzen, um Informationsaustausch und Krisenmanagement zu vereinfachen. Zudem dient er zur Unterstützung des geplanten Europäischen Programms zum Schutz kritischer Infrastrukturen.

[137] «Act of 3 February 2005»

3. Vorschlag für einen Beschluss des Rates über die Unterzeichnung der Konvention 198 des Europarates über Geldwäsche, Terrorismusfinanzierung sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten:

   Der Vorschlag regt die 46 Mitgliederländer an, dass sie die gleichen strengen Vorschriften gegen die Geldwäsche einführen, wie sie bereits in der EU gelten und eine einheitliche Front im Kampf gegen die Terrorismusfinanzierung bilden.

4. Mitteilung «Rekrutierung von Terroristen: Bekämpfung der Ursachen von Radikalisierung und Gewaltbereitschaft»:

   Die Mitteilung ist der im Haager Programm vorgesehene Beitrag der Kommission für diesen Bereich. Der Rat muss bis Ende Jahr eine Strategie ausarbeiten. In ihr werden mögliche Lösungen für ein effizientes Herangehen an diese Frage in unterschiedlichen Bereichen wie Internet, Zusammenarbeit zwischen den Strafverfolgungsbehörden und Geheimdiensten der Mitgliedstaaten und Aussenbeziehungen vorgeschlagen.

Die EU hat am 20. September 2005 [2005/671/JI] einen Beschluss über den Informationsaustausch und die Zusammenarbeit betreffend terroristische Straftaten erlassen. Schliesslich hat die EU-Kommission im Rahmen des Haager Programms zehn Prioritäten für die nächsten fünf Jahre ausgearbeitet [KOM(2005) 184], darunter ein Programm zur Bekämpfung des Terrorismus.